

通信方法、装置及系统

技术领域

5 本申请涉及通信技术领域，尤其涉及通信方法、装置及系统。

背景技术

10 传统的移动网络中，终端设备之间的信令通信和数据通信路径需要经过网络侧设备（如基站/服务网关（serving gateway, SGW）/分组数据网关（packet data network gateway, PGW））。不同的终端设备之间是不能直接进行通信的。即使两个距离很近的终端设备之间，以终端设备 1 和终端设备 2 为例，在进行数据传递时，也需要终端设备 1 先将数据发送给连接的基站 1，进而数据经过网络侧的传输到达终端设备 2 连接的基站 2（此时基站 1 和基站 2 可以为相同基站，也可为不同基站），最后由基站 2 将数据发送给终端设备 2，这样会对网络传输带宽有较大的需求量，并且传输效率较低。

15 在设备到设备通信（device-to-device, D2D）需要短距离直连通信的需求下，临近业务（proximity-based services, ProSe）课题被提出。ProSe 要求终端设备之间直接进行数据交换，或者仅通过基站而不经核心网设备（如 SGW/PGW）进行数据交换，因此可以提高距离较近的终端设备之间的通信效率。

20 随着 ProSe 技术的发展，ProSe 课题引入基于终端设备之间短距离直连通信的 PC5 接口，使得终端设备之间的数据和信令传输可以不再经过基站的转发。由于终端设备之间通过 PC5 接口直连通信，类比于终端设备与基站之间依赖 Uu 接口的 Uu 通信，因此终端设备之间通过 PC5 接口直连通信又可以称为 PC5 单播通信。

25 目前，ProSe 技术建立终端设备之间的单播数据交换前，需要按顺序执行 ProSe 发现流程和 PC5 单播建立流程。其中，ProSe 发现流程用于实现两个终端设备之间的彼此发现，PC5 单播建立流程用于建立两个终端设备之间通过 PC5 接口直连通信的信令连接与数据连接。在第四代（4th generation, 4G）通信技术中，由于 PC5 单播建立流程中无需安全协商流程，终端设备之间默认使用匹配的安全参数保护 ProSe 单播通信，因此在 PC5 单播建立流程不会因为安全参数的不一致导致 PC5 单播建立失败。然而，在第五代（5th generation, 5G）通信技术中，短距离直连通信业务被用于车联网（vehicle-to-everything, V2X）中。V2X 场景将安全协商引入 PC5 单播建立流程，两端终端设备的安全参数的不一致将会导致 PC5 单播建立失败。

发明内容

30 本申请实施例提供通信方法、装置及系统，用于解决 V2X 场景将安全协商引入 PC5 单播建立流程，两端终端设备的安全参数的不一致将会导致 PC5 单播建立失败的问题。

 为达到上述目的，本申请的实施例采用如下技术方案：

 第一方面，提供了一种通信方法，该方法包括：第一直连通信发现名称管理功能网元获取第一终端设备的安全参数，该安全参数为建立该第一终端设备与第二终端设备之间的 PC5 连接所需的安全参数；第一直连通信发现名称管理功能网元接收来自第

二直连通信发现名称管理功能网元的该第二终端设备的安全参数；第一直连通信发现名称管理功能网元根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信。现有的 V2X 场景将安全协商引入 PC5 单播建立流程，两端终端设备的安全参数的不一致将会导致 PC5 单播建立失败。

- 5 此时由于已经完成 ProSe 发现流程，也执行了 PC5 单播建立流程的部分步骤，因此将造成过多的信令浪费。本申请实施例可以在 ProSe 发现流程中对第一终端设备的安全参数与第二终端设备的安全参数进行匹配，并根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信。进而，若第一终端设备与第二终端设备不支持互相通信，可以及时终止当前的 ProSe 发现流程，因此可以避免现有技术中在 ProSe 发现流程之后的 PC5 单播建立流程中，
10 两端终端设备的安全参数的不一致导致 PC5 单播建立失败所带来的信令浪费的问题。

- 在一种可能的实现方式中，第一直连通信发现名称管理功能网元根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信，包括：当第一终端设备的安全参数和第二终端设备的安全参数
15 不匹配时，第一直连通信发现名称管理功能网元确定第一终端设备和第二终端设备不支持互相通信。

- 在一种可能的实现方式中，本申请实施例提供的通信方法还包括：第一直连通信发现名称管理功能网元发送第一指示信息，该第一指示信息用于指示第一终端设备与第二终端设备不支持互相通信。这样，第一终端设备可以确定不支持与第二终端设备
20 互相通信，或者第二终端设备可以确定不支持与第一终端设备互相通信，从而可以及时终止当前的 ProSe 发现流程，避免现有技术中在 ProSe 发现流程之后的 PC5 单播建立流程中，两端终端设备的安全参数的不一致导致 PC5 单播建立失败所带来的信令浪费的问题。

- 在一种可能的实现方式中，第一直连通信发现名称管理功能网元根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信，包括：当第一终端设备的安全参数和第二终端设备的安全参数
25 匹配时，第一直连通信发现名称管理功能网元确定第一终端设备和第二终端设备支持互相通信。

- 在一种可能的实现方式中，本申请实施例提供的通信方法还包括：第一直连通信发现名称管理功能网元发送第二指示信息，该第二指示信息用于指示第一终端设备和第二终端设备支持互相通信。这样，第一终端设备可以确定支持与第二终端设备互相
30 通信，或者第二终端设备可以确定支持与第一终端设备互相通信，从而可以继续当前的 ProSe 发现流程，避免现有技术中在 ProSe 发现流程之后的 PC5 单播建立流程中，两端终端设备的安全参数的不一致导致 PC5 单播建立失败所带来的信令浪费的问题。

- 35 在一种可能的实现方式中，本申请实施例提供的通信方法还包括：第一直连通信发现名称管理功能网元向第一终端设备发送发现响应，发现响应包括业务发现使用的发现参数。基于该方案，第一终端设备接收到发现响应之后，可以确定支持与第二终端设备互相通信。也就是说，第一终端设备可以认为第一终端设备的安全参数和第二终端设备的安全参数匹配，从而可以继续后续的 ProSe 发现流程，避免了现有技术中

在 ProSe 发现流程之后的 PC5 单播建立流程中，两端终端设备的安全参数的不一致导致 PC5 单播建立失败所带来的信令浪费的问题。

在一种可能的实现方式中，本申请实施例提供的通信方法还包括：该第一直连通信发现名称管理功能网元向第一终端设备发送该第一终端设备的安全参数。基于该方案，第一终端设备可以获取自己的安全参数。

在一种可能的实现方式中，本申请实施例中的安全参数包括安全策略，和/或安全能力。

在一种可能的实现方式中，本申请实施例中的安全参数包括安全能力；第一直连通信发现名称管理功能网元获取该第一终端设备的安全参数，包括：第一直连通信发现名称管理功能网元接收来自对应的移动管理网元的该第一终端设备的安全能力；或者，第一直连通信发现名称管理功能网元接收来自第一终端设备的该第一终端设备的安全能力。也就是说，本申请实施例中，第一直连通信发现名称管理功能网元不仅可以从第一终端设备获取第一终端设备的安全能力，还可以从网络侧获取第一终端设备的安全能力。

在一种可能的实现方式中，本申请实施例中的安全参数包括安全策略；第一直连通信发现名称管理功能网元获取第一终端设备的安全参数，包括：第一直连通信发现名称管理功能网元接收来自该第一终端设备的该第一终端设备的安全策略；或者，第一直连通信发现名称管理功能网元从对应的策略控制网元获取该第一终端设备的安全策略；或者，第一直连通信发现名称管理功能网元从对应的统一数据管理网元获取该第一终端设备的安全策略。也就是说，本申请实施例中，第一直连通信发现名称管理功能网元不仅可以从第一终端设备获取第一终端设备的安全策略，还可以从网络侧获取第一终端设备的安全策略。

在一种可能的实现方式中，本申请实施例中的安全策略包括该 PC5 连接中的用户面机密性保护策略和完整性保护策略。基于该安全策略，可以实现 PC5 连接中的用户面的安全保护。

在一种可能的实现方式中，本申请实施例中的安全能力包括该 PC5 连接中支持的一个或者多个机密性保护算法和完整性保护算法。基于该安全策略，可以实现 PC5 连接中的控制面和/或用户面的安全保护。

第二方面，提供了一种通信装置用于实现上述方法。该通信装置可以为上述第一方面中的第一直连通信发现名称管理功能网元，或者包含上述第一直连通信发现名称管理功能网元的装置。该通信装置包括实现上述方法相应的模块、单元、或手段 (means)，该模块、单元、或 means 可以通过硬件实现，软件实现，或者通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块或单元。

第三方面，提供了一种通信装置，包括：处理器和存储器；该存储器用于存储计算机指令，当该处理器执行该指令时，以使该通信装置执行上述第一方面所述的方法。该通信装置可以为上述第一方面中的第一直连通信发现名称管理功能网元，或者包含上述第一直连通信发现名称管理功能网元的装置。

第四方面，提供了一种通信装置，包括：处理器；该处理器用于与存储器耦合，并读取存储器中的指令之后，根据该指令执行如上述第一方面所述的方法。该通信装

置可以为上述第一方面中的第一直连通信发现名称管理功能网元，或者包含上述第一直连通信发现名称管理功能网元的装置。

第五方面，提供了一种通信装置，包括：处理器接口电路；接口电路，用于接收计算机程序或指令并传输至处理器；处理器用于执行所述计算机程序或指令，以使该通信装置执行如上述第一方面所述的方法。

第六方面，提供了一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机可以执行上述第一方面所述的方法。

第七方面，提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机可以执行上述第一方面所述的方法。

第八方面，提供了一种通信装置（例如，该通信装置可以是芯片或芯片系统），该通信装置包括处理器，用于实现上述第一方面中所涉及的功能。在一种可能的实现方式中，该通信装置还包括存储器，该存储器，用于保存必要的程序指令和数据。该通信装置是芯片系统时，可以由芯片构成，也可以包含芯片和其他分立器件。

其中，第二方面至第八方面中任一种可能的实现方式所带来的技术效果可参见上述第一方面中不同设计方式所带来的技术效果，此处不再赘述。

第九方面，提供了一种通信系统，该通信系统包括第一直连通信发现名称管理功能网元和第二直连通信发现名称管理功能网元。其中，第一直连通信发现名称管理功能网元，用于获取第一终端设备的安全参数，该安全参数为建立第一终端设备与第二终端设备之间的 PC5 连接所需的安全参数。第二直连通信发现名称管理功能网元，用于获取第二终端设备的安全参数，并向第一直连通信发现名称管理功能网元发送第二终端设备的安全参数；第一直连通信发现名称管理功能网元，还用于接收来自第二直连通信发现名称管理功能网元的第二终端设备的安全参数，并根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信。其中，第八方面的技术效果可参考上述第一方面，在此不再赘述。

附图说明

图 1 为本申请实施例提供的一种通信系统的结构示意图；

图 2 为本申请实施例提供的一种 5G 网络中 ProSe 控制面架构示意图；

图 3 为本申请实施例提供的通信设备的结构示意图；

图 4 为本申请实施例提供的一种通信方法的交互示意图；

图 5 为本申请实施例提供的另一种通信方法的交互示意图；

图 6 为本申请实施例提供的又一种通信方法的交互示意图；

图 7 为本申请实施例提供的一种通信方法的流程示意图；

图 8 为本申请实施例提供的通信装置的结构示意图。

具体实施方式

为了方便理解本申请实施例的技术方案，首先给出本申请相关技术的简要介绍如下。

第一，发现类型（discovery type）：

本申请实施例中，发现类型包括开放发现（open discovery）或者限制发现（restricted discovery）。open discovery 与 restricted discovery 的相关描述可参考现有的第三代合

作伙伴计划 (3rd generation partnership project, 3GPP) 技术标准 (technical standards, TS) 23.303, v15.1.0, 在此不予赘述。举个例子, 比如一个终端设备自己打游戏, 没有明确的游戏伙伴, 则他可以发起一个开放发现, “随机”找到一个游戏伙伴就行。而若终端设备打游戏有明确的伙伴, 则他可以通过限制发现来“指定”一个伙伴, 只有他指定的伙伴才能接入游戏, 其他的则不行。因此, 开放发现就如摇一摇应用, 可以随意的摇到开起了摇一摇应用的另一个用户。限制发现则如面对面建群, 只有知道群号的用户才可以接入。

第二, 发现模式 (discovery mode) :

在现有 4G ProSe 标准中 (3GPP TS 23.303, v15.1.0), 定义了模式 A (Model A) 或模式 B (Model B)。Model A 和 Model B 的区别在于发起 discovery 的方式不同。Model A 的含义是“我在这”, Model A 发现流程中两端终端设备分为播报方用户设备 (user equipment, UE) (announcing UE) 和监听方 UE (monitoring UE), announcing UE 广播“我在这”, monitoring UE 接收到 announcing UE 广播的消息后根据是否符合自己业务需求确定是否与 announcing UE 建立临近业务的连接。Model B 的含义是“谁在那? /你在哪?”, Model B 发现流程中两端终端设备分为被发现者 UE (discoveree UE) 和发现者 UE (discoverer UE), discoverer UE 发起特定业务请求, 请求中包括特定的信息, 就是问“谁在那? /你在哪?”, discoveree UE 接收到 discoverer UE 发起的业务请求之后根据自己是否可以提供业务服务来确定是否回复该请求消息, 若回复响应消息, 说明“我在这”。其中, 本申请实施例以 open discovery 场景适用于 model A 发现模型, 而 restricted discovery 场景适用于 model A 和 model B 两种发现模型为例进行说明, 在此统一说明, 以下不再赘述。

第三, 发现命令 (discovery command) :

本申请实施例中, 发现命令用于告知网络侧互相通信的两个终端设备是 announcing UE 还是 monitoring UE; 是响应终端设备 (response UE) 还是请求终端设备 (query UE)。其中, announcing UE 与 monitoring UE 为上述 Model A 发现流程中的两端终端设备, response UE 与 query UE 分别对应上述 Model B 发现流程中的 discoveree UE 和 discoverer UE, 在此统一说明, 以下不再赘述。

第四, 用于 ProSe 业务的 user identity:

本申请实施例中, 用于 ProSe 业务的 user identity 可以是临近业务应用标识 (ProSe application ID), 或者是限制临近业务应用用户标识 (restricted ProSe application user ID, RPAUID) 或者是临近发现 UE 标识 (ProSe discovery UE ID, PDUID) 等。其中, 本申请实施例以 ProSe application ID 用于开放发现 (open discovery) 场景, PDUID 或 RPAUID 用于限制发现 (restricted discovery) 场景为例进行说明, 在此统一说明, 以下不再赘述。

第五, 安全策略与安全策略匹配:

安全策略是用于描述是否开启安全保护的策略, 可用于确定安全保护方法。本申请实施例中用于不同场景的安全策略包括以下至少一种:

PC5 连接中的控制面机密性保护策略;

PC5 连接中的控制面完整性保护策略;

PC5 连接中的用户面机密性保护策略；

或者，PC5 连接中的用户面完整性保护策略。

其中，控制面机密性保护即保护信令在传输过程中的机密性；控制面完整性保护即保护信令在传输过程中的完整性；用户面机密性保护即保护用户面数据在传输过程中的机密性；用户面完整性保护即保护用户面数据在传输过程中的完整。本申请实施例中，完整性是指获取到的信令或数据与原始的信令或数据一致，没有被修改，因此，完整性保护是为了使得攻击者“攻击不成”。机密性是指无法被直接看出真实内容，因此机密性保护是为了使得攻击者“读不懂”。此外，本申请实施例中的机密性保护也可以称为加密保护，在此统一说明，以下不再赘述。

本申请实施例中，PC5 连接中的控制面机密性保护策略与 PC5 连接中的控制面完整性保护策略属于 PC5 连接中的控制面安全策略；PC5 连接中的用户面机密性保护策略与 PC5 连接中的用户面完整性保护策略属于 PC5 连接中的用户面安全策略，在此统一说明，以下不再赘述。

本申请实施例中，保护策略共分有开启（REQUIRED），不开启（NOT NEEDED）和可选（PREFERRED）三种。REQUIRED 为需要开启安全，NOT NEEDED 为不需要开启安全，PREFERRED 偏好开启，即可以开启安全但也可以不开启安全，在此统一说明，以下不再赘述。

示例性的，以 PC5 连接中的控制面机密性保护策略为例，则 PC5 连接中的控制面机密性保护策略包括：PC5 连接中的控制面机密性保护开启（REQUIRED）、PC5 连接中的控制面机密性保护不开启（NOT NEEDED）、或者 PC5 连接中的控制面机密性保护可选（PREFERRED）。PC5 连接中的控制面机密性保护策略、PC5 连接中的用户面机密性保护策略、或者 PC5 连接中的用户面完整性保护策略的示例可参考 PC5 连接中的控制面机密性保护策略的示例，在此不再赘述。

需要说明的是，本申请实施例中，安全策略在被发送时，一般情况下只会选择三种（REQUIRED、NOT NEEDED 和 PREFERRED）中的一种发送，在某些特殊的场景下可能会选择至少 2 种发送，并且其中一个是 PREFERRED。比如，在发送 NOT NEEDED 和 PREFERRED 时，代表倾向不开启安全保护；在发送 REQUIRED 和 PREFERRED 时，则代表倾向开启安全保护。

本申请实施例中，对于安全策略中的某种保护策略，假设一个终端设备的保护策略为保护开启（REQUIRED），另一个终端设备的保护策略为保护不开启（NOT NEEDED），则可以认为这两个终端设备的这种保护策略不匹配，否则可以认为这两个终端设备的这种保护策略匹配。

示例性的，以 PC5 连接中的用户面机密性保护为例，假设第一终端设备在 PC5 连接中的用户面机密性保护策略为不开启（NOT NEEDED），第二终端设备在 PC5 连接中的用户面机密性保护策略为开启（REQUIRED）；或者，假设第一终端设备在 PC5 连接中的用户面机密性保护策略为开启（REQUIRED），第二终端设备在 PC5 连接中的用户面机密性保护策略为不开启（NOT NEEDED），则可以确定第一终端设备与第二终端设备在 PC5 连接中的用户面机密性保护策略不匹配，其他情况可以视为第一终端设备与第二终端设备在 PC5 连接中的用户面机密性保护策略匹配。

一种可能的实现方式中，本申请实施例中，当安全策略包括一种保护策略时，安全策略匹配是指该保护策略匹配。比如，假设安全策略仅包括 PC5 连接中的用户面机密性保护策略，则只要 PC5 连接中的用户面机密性保护策略匹配，则可以认为安全策略匹配。

5 另一种可能的实现方式中，本申请实施例中，当安全策略包括多种保护策略时，安全策略匹配是指这多种保护策略中的每种保护策略均匹配。比如，假设安全策略包括 PC5 连接中的用户面机密性保护策略和完整性保护策略，则当 PC5 连接中的用户面机密性保护策略匹配，并且 PC5 连接中的用户面完整性保护策略匹配时，可以认为安全策略匹配；否则认为安全策略不匹配。

10 需要说明的是，本申请实施例中，PC5 连接中的控制面机密性保护策略、PC5 连接中的控制面完整性保护策略、PC5 连接中的用户面机密性保护策略；或者，PC5 连接中的用户面完整性保护策略中的多种保护策略可以相同，本申请实施例对此不做具体限定。

第六，安全能力与安全能力匹配：

15 本申请实施例中的安全能力包括以下至少一种：

PC5 连接中支持的一个或者多个控制面机密性保护算法；

PC5 连接中支持的一个或者多个控制面完整性保护算法；

PC5 连接中支持的一个或者多个用户面机密性保护算法；

或者，PC5 连接中支持的一个或者多个用户面完整性保护算法。

20 其中，PC5 连接中支持的一个或者多个控制面机密性保护算法与 PC5 连接中支持的一个或者多个控制面完整性保护算法属于 PC5 连接中的控制面安全能力；PC5 连接中支持的一个或者多个用户面机密性保护算法与 PC5 连接中支持的一个或者多个用户面完整性保护算法属于 PC5 连接中的用户面安全能力，在此统一说明，以下不再赘述。

25 本申请实施例中，对于安全能力中的某种保护算法，假设一个终端设备在 PC5 连接中支持的一个或者多个保护算法与另一个终端设备在 PC5 连接中支持的一个或者多个保护算法存在共同的算法，则可以认为这两个终端设备的这种保护算法匹配，否则可以认为这两个终端设备的这种保护算法不匹配。

30 示例性的，以 PC5 连接中的用户面机密性保护为例，假设第一终端设备在 PC5 连接中的用户面机密性保护算法为 NEA0、NEA1 和 NEA2，第二终端设备在 PC5 连接中的用户面机密性保护算法为 NEA1 和 NEA2，则此时两终端设备的在 PC5 连接中的用户面机密性保护算法的共同项为 NEA1 和 NEA2，即存在共同项，进而可以确定第一终端设备与第二终端设备在 PC5 连接中的用户面机密性保护算法匹配，否则确定第一终端设备与第二终端设备在 PC5 连接中的用户面机密性保护算法不匹配。

35 一种可能的实现方式中，本申请实施例中，当安全能力包括一种保护算法时，安全能力匹配是指该保护算法匹配。比如，假设安全能力仅包括 PC5 连接中的用户面机密性保护算法，则只要 PC5 连接中的用户面机密性保护算法匹配，则可以认为安全能力匹配。

另一种可能的实现方式中，本申请实施例中，当安全能力包括多种保护算法时，安全能力匹配是指这多种保护算法中的每种保护算法均匹配。比如，假设安全能力包

括 PC5 连接中的用户面机密性保护算法和完整性保护算法,则当 PC5 连接中的用户面机密性保护算法匹配,并且 PC5 连接中的用户面完整性保护算法匹配时,可以认为安全能力匹配;否则认为安全能力不匹配。

需要说明的是,本申请实施例中,PC5 连接中支持的一个或者多个控制面机密性保护算法、PC5 连接中支持的一个或者多个控制面完整性保护算法、PC5 连接中支持的一个或者多个用户面机密性保护算法、或者 PC5 连接中支持的一个或者多个用户面完整性保护算法中的多种保护算法可以相同或者存在共同项,本申请实施例对此不做具体限定。

第七,安全保护方法:

本申请实施例中的安全保护方法分为以下三类:

1、ProSe 发现流程中第一条 PC5 广播消息所使用的安全保护方法,用于保护 ProSe 发现流程中第一条 PC5 广播消息。

2、PC5 连接的控制面使用的安全保护方法,用于保护 PC5 连接的控制面信令。

3、PC5 连接的用户面使用的安全保护方法,用于保护 PC5 连接的用户面数据。

本申请实施例中,安全保护方法包括机密性保护和/或完整性保护是否开启,在此统一说明,以下不再赘述。

示例性的,第一条 PC5 广播消息所使用的安全保护方法例如可以包括第一条 PC5 广播消息的机密性保护和/或完整性保护是否开启;或者,PC5 连接的控制面使用的安全保护方法例如可以包括 PC5 连接的控制面的机密性保护和/或完整性保护是否开启;或者,PC5 连接的用户面使用的安全保护方法例如可以包括 PC5 连接的用户面的机密性保护和/或完整性保护是否开启。

需要说明的是,本申请实施例中,PC5 连接的控制面使用的安全保护方法与 PC5 连接的用户面使用的安全保护方法属于 PC5 连接的安全保护方法,在此统一说明,以下不再赘述。

下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行描述。其中,在本申请的描述中,除非另有说明,“/”表示前后关联的对象是一种“或”的关系,例如,A/B 可以表示 A 或 B;本申请中的“和/或”仅仅是一种描述关联对象的关联关系,表示可以存在三种关系,例如,A 和/或 B,可以表示:单独存在 A,同时存在 A 和 B,单独存在 B 这三种情况,其中 A,B 可以是单数或者复数。并且,在本申请的描述中,除非另有说明,“多个”是指两个或两个以上。“以下至少一项(个)”或其类似表达,是指的这些项中的任意组合,包括单项(个)或复数项(个)的任意组合。例如,a,b,或 c 中的至少一项(个),可以表示:a,b,c,a-b,a-c,b-c,或 a-b-c,其中 a,b,c 可以是单个,也可以是多个。另外,为了便于清楚描述本申请实施例的技术方案,在本申请的实施例中,采用了“第一”、“第二”等字样对功能和作用基本相同的相同项或相似项进行区分。本领域技术人员可以理解“第一”、“第二”等字样并不对数量和执行次序进行限定,并且“第一”、“第二”等字样也并不限定一定不同。同时,在本申请实施例中,“示例性的”或者“例如”等词用于表示作例子、例证或说明。本申请实施例中被描述为“示例性的”或者“例如”的任何实施例或设计方案不应被解释为比其它实施例或设计方案更优选或更具优势。确切而言,使用“示例性的”或者“例如”等词旨在以

具体方式呈现相关概念，便于理解。

此外，本申请实施例描述的网络架构以及业务场景是为了更加清楚的说明本申请实施例的技术方案，并不构成对于本申请实施例提供的技术方案的限定，本领域普通技术人员可知，随着网络架构的演变和新业务场景的出现，本申请实施例提供的技术方案对于类似的技术问题，同样适用。

如图 1 所示，为本申请实施例提供的一种通信系统 10。该通信系统 10 包括第一直连通信发现名称管理功能网元 101 和第二直连通信发现名称管理功能网元 102。该第一直连通信发现名称管理功能网元 101 和第二直连通信发现名称管理功能网元 102 之间可以直接通信，也可以通过其他设备的转发进行通信，本申请实施例对此不做具体限定。

其中，第一直连通信发现名称管理功能网元 101，用于获取第一终端设备的安全参数，该安全参数为建立第一终端设备与第二终端设备之间的 PC5 连接所需的安全参数。

第二直连通信发现名称管理功能网元 102，用于获取第二终端设备的安全参数，并向第一直连通信发现名称管理功能网元 101 发送第二终端设备的安全参数。

第一直连通信发现名称管理功能网元 101，还用于接收来自第二直连通信发现名称管理功能网元 102 的第二终端设备的安全参数，并根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信。其中，该方案的具体实现将在后续方法实施例中详细描述，在此不予赘述。

现有的 V2X 场景将安全协商引入 PC5 单播建立流程，两端终端设备的安全参数的不一致将会导致 PC5 单播建立失败。此时由于已经完成 ProSe 发现流程，也执行了 PC5 单播建立流程的部分步骤，因此将造成过多的信令浪费。本申请实施例可以在 ProSe 发现流程中对第一终端设备的安全参数与第二终端设备的安全参数进行匹配，并根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信。进而，若第一终端设备与第二终端设备不支持互相通信，可以及时终止当前的 ProSe 发现流程，因此可以避免现有技术中在 ProSe 发现流程之后的 PC5 单播建立流程中，两端终端设备的安全参数的不一致导致 PC5 单播建立失败所带来的信令浪费的问题。其中，本申请实施例中的安全参数包括安全策略和/或安全能力，在此统一说明，以下不再赘述。

可选的，图 1 所示的通信系统 10 可以适用于目前正在讨论的 5G 网络，也可以适用于未来的其他网络等，本申请实施例对此不做具体限定。

示例性的，以图 1 所示的通信系统 10 适用于目前正在讨论的 5G 网络为例，则本申请实施例中的直连通信发现名称管理功能网元（包括第一直连通信发现名称管理功能网元 101 和第二直连通信发现名称管理功能网元 102）所对应的网元或者实体可以为该 5G 网络中的直连通信发现名称管理功能（direct discovery name management function, DDNMF）网元。

如图 2 所示，为本申请实施例提供的一种 5G 网络中 ProSe 控制面架构示意图，包括一个或多个终端设备（图 2 以包括终端设备 1、终端设备 2、终端设备 3 与终端设备 4 为例进行示意）、下一代无线接入网络（next generation-radio access network, NG-RAN）

设备、统一数据存储 (unified data repository, UDR) 网元、统一数据管理 (unified data management, UDM) 网元、会话管理功能 (session management function, SMF) 网元、接入和移动性管理功能 (access and mobility management function, AMF) 网元、网络开放功能 (network exposure function, NEF) 网元、策略控制功能 (policy control function, PCF) 网元、用户面功能 (user plane function, UPF) 网元、5G DDNMF 网元以及数据网络 (data network, DN)。

其中, 与传统蜂窝网络通信相比, 可以用于 ProSe 通信的终端设备需要有临近业务应用 (ProSe application) 功能, 具有 ProSe 应用功能的终端设备之间通过 PC5 口通信。与 ProSe 应用相对应的是 ProSe 应用服务器。ProSe 应用服务器可以是 DN 中的应用功能 (application function, AF) 网元。具有 ProSe 应用服务器功能的 AF 具有 23.501 R-15 版本中定义的 AF 的所有功能, 以及用于 ProSe 业务的相关功能。也就是说, 在 5G 网络中 ProSe 控制面架构中, ProSe 应用服务器与终端设备是通过终端设备-NG-RAN 设备-UPF 网元-AF 网元的路径进行用户面通信。此外, ProSe 应用服务器还可以通过 NEF 与 5G 核心网 (5G core network, 5GC) 中的其他网络功能 (network function, NF) 进行通信, 比如通过 NEF 网元与 PCF 网元通信。

本申请实施例中, DDNMF 网元具有为开放临近业务直连发现 (open ProSe direct discovery) 分配和处理临近业务应用标识 (ProSe application ID) 与 ProSe 发现使用的 code 之间映射关系的作用。在限制性临近业务直连发现 (restricted ProSe direct discovery) 中, DDNMF 网元与 ProSe 应用服务器通过 PC2 口通信, 用于处理发现请求的授权。

此外, AMF 网元、UDR 网元、SMF 网元、UPF 网元、UDM 网元、NEF 网元或者 PCF 网元的相关描述可参考现有的 3GPP 5G 标准, 在此不予赘述。

可选的, 本申请实施例中的终端设备, 可以是用于实现无线通信功能的设备, 例如终端或者可用于终端中的芯片等, 其可以部署在陆地上, 包括室内或室外、手持或车载; 也可以部署在水面上 (如轮船等); 还可以部署在空中 (例如飞机、气球和卫星上等)。其中, 终端可以是 5G 网络或者未来演进的公共陆地移动网 (public land mobile network, PLMN) 中的 UE、接入终端、终端单元、终端站、移动站、移动台、远方站、远程终端、移动设备、无线通信设备、终端代理或终端装置等。接入终端可以是蜂窝电话、无绳电话、会话启动协议 (session initiation protocol, SIP) 电话、无线本地环路 (wireless local loop, WLL) 站、个人数字助理 (personal digital assistant, PDA)、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备或可穿戴设备, 无人机 (unmanned aerial vehicle, UAV) 和无人机控制器 (UAV controller, UAVC), 虚拟现实 (virtual reality, VR) 终端设备、增强现实 (augmented reality, AR) 终端设备、工业控制 (industrial control) 中的无线终端、无人驾驶 (self driving) 中的无线终端、远程医疗 (remote medical) 中的无线终端、智能电网 (smart grid) 中的无线终端、运输安全 (transportation safety) 中的无线终端、智慧城市 (smart city) 中的无线终端、智慧家庭 (smart home) 中的无线终端等。终端可以是移动的, 也可以是固定的。

可选的, 本申请实施例中的 RAN 设备, 是一种为终端设备提供无线通信功能的设

备。接入网设备例如包括但不限于：5G中的下一代基站(gnodeB, gNB)、演进型节点B (evolved node B, eNB)、无线网络控制器 (radio network controller, RNC)、节点B (node B, NB)、基站控制器 (base station controller, BSC)、基站收发台 (base transceiver station, BTS)、家庭基站 (例如, home evolved nodeB, 或 home node B, HNB)、基带单元 (baseBand unit, BBU)、传输点(transmitting and receiving point, TRP)、发射点(transmitting point, TP)、移动交换中心等。

可选的, 本申请实施例中的第一直连通信发现名称管理功能网元与第二直连通信发现名称管理功能网元也可以称之为通信装置, 其可以是一个通用设备或者是一个专用设备, 本申请实施例对此不作具体限定。

10 可选的, 本申请实施例中的第一直连通信发现名称管理功能网元与第二直连通信发现名称管理功能网元的相关功能可以由一个设备实现, 也可以由多个设备共同实现, 还可以是由一个设备内的一个或多个功能模块实现, 本申请实施例对此不作具体限定。可以理解的是, 上述功能既可以是硬件设备中的网络元件, 也可以是在专用硬件上运行的软件功能, 或者是硬件与软件的结合, 或者是平台(例如, 云平台)上实例化的虚拟化功能。

15 例如, 本申请实施例中的第一直连通信发现名称管理功能网元与第二直连通信发现名称管理功能网元的相关功能可以通过图3中的通信设备300来实现。图3所示为本申请实施例提供的通信设备300的结构示意图。该通信设备300包括一个或多个处理器301, 通信线路302, 以及至少一个通信接口(图3中仅是示例性的以包括通信接口304, 以及一个处理器301为例进行说明), 可选的还可以包括存储器303。

处理器301可以是一个通用中央处理器 (central processing unit, CPU), 微处理器, 特定应用集成电路 (application-specific integrated circuit, ASIC), 或一个或多个用于控制本申请方案程序执行的集成电路。

通信线路302可包括一通路, 用于连接不同组件之间。

25 通信接口304, 可以是收发模块用于与其他设备或通信网络通信, 如以太网, RAN, 无线局域网(wireless local area networks, WLAN)等。例如, 所述收发模块可以是收发器、收发机一类的装置。可选的, 所述通信接口304也可以是位于处理器301内的收发电路, 用以实现处理器的信号输入和信号输出。

30 存储器303可以是具有存储功能的装置。例如可以是只读存储器 (read-only memory, ROM) 或可存储静态信息和指令的其他类型的静态存储设备, 随机存取存储器 (random access memory, RAM) 或者可存储信息和指令的其他类型的动态存储设备, 也可以是电可擦可编程只读存储器 (electrically erasable programmable read-only memory, EEPROM)、只读光盘 (compact disc read-only memory, CD-ROM) 或其他光盘存储、光碟存储 (包括压缩光碟、激光碟、光碟、数字通用光碟、蓝光光碟等)、35 磁盘存储介质或者其他磁存储设备、或者能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质, 但不限于此。存储器可以是独立存在, 通过通信线路302与处理器相连接。存储器也可以和处理器集成在一起。

其中, 存储器303用于存储执行本申请方案的计算机执行指令, 并由处理器301来控制执行。处理器301用于执行存储器303中存储的计算机执行指令, 从而实现本

申请实施例中提供的通信方法。

或者，可选的，本申请实施例中，也可以是处理器 301 执行本申请下述实施例提供的通信方法中的处理相关的功能，通信接口 304 负责与其他设备或通信网络通信，本申请实施例对此不作具体限定。

- 5 可选的，本申请实施例中的计算机执行指令也可以称之为应用程序代码，本申请实施例对此不作具体限定。

在具体实现中，作为一种实施例，处理器 301 可以包括一个或多个 CPU，例如图 3 中的 CPU0 和 CPU1。

- 10 在具体实现中，作为一种实施例，通信设备 300 可以包括多个处理器，例如图 3 中的处理器 301 和处理器 308。这些处理器中的每一个可以是一个单核（single-core）处理器，也可以是一个多核（multi-core）处理器。这里的处理器可以包括但不限于以下至少一种：中央处理单元（central processing unit，CPU）、微处理器、数字信号处理器（DSP）、微控制器（microcontroller unit，MCU）、或人工智能处理器等各类运行软件的计算设备，每种计算设备可包括一个或多个用于执行软件指令以进行运算或
15 处理的核。

- 在具体实现中，作为一种实施例，通信设备 300 还可以包括输出设备 305 和输入设备 306。输出设备 305 和处理器 301 通信，可以以多种方式来显示信息。例如，输出设备 305 可以是液晶显示器（liquid crystal display，LCD）、发光二极管（light emitting diode，LED）显示设备，阴极射线管（cathode ray tube，CRT）显示设备，或投影仪（projector）等。输入设备 306 和处理器 301 通信，可以以多种方式接收用户的输入。
20 例如，输入设备 306 可以是鼠标、键盘、触摸屏设备或传感设备等。

- 上述的通信设备 300 有时也可以称为通信装置，其可以是一个通用设备或者是一个专用设备。例如通信设备 300 可以是台式机、便携式电脑、网络服务器、掌上电脑（personal digital assistant，PDA）、移动手机、平板电脑、无线终端设备、嵌入式设备、上述终端设备、上述网络设备、或具有图 3 中类似结构的设备。本申请实施例不限定通信设备 300 的类型。
25

下面将结合附图，对本申请实施例提供的通信方法进行示例性说明。

- 需要说明的是，本申请下述实施例中各个网元之间的消息名字或消息中各参数的名字等只是一个示例，具体实现中也可以是其他的名字，本申请实施例对此不作具体
30 限定。

示例性的，本申请实施例提供一种通信方法，该通信方法以图 2 所示的 5G 网络中 ProSe 控制面架构为例，依托 restricted discovery 的发现场景，借助 ProSe 发现流程中的发现参数获取流程进行安全参数的匹配。如图 4 所示，该通信方法包括如下步骤：

- S401、终端设备 1 向 AMF1 网元发送发现请求（discovery request）1。相应的，
35 AMF1 网元接收来自终端设备 1 的发现请求 1。其中，该发现请求 1 包括终端设备 1 的 3GPP 身份信息、用于 ProSe 业务的身份信息（user identity）、发现模式、发现命令、发现类型和应用标识（application ID）中的一个或多个。

可选的，本申请实施例中，终端设备 1 的 3GPP 身份信息例如可以为签约隐藏标识（subscription concealed identifier，SUCI）、5G-全球唯一临时标识（global unique

temporary identifier, GUTI)、通用公共用户标识符(generic public subscription identifier, GPSI)、永久设备标识符(permanent equipment identifier, PEI)中的一个。

其中,发现类型、发现模式、发现命令或者用于 ProSe 业务的 user identity 的相关描述可参考具体实施方式前序介绍部分,在此不再赘述。

5 可选的,本申请实施例中的发现请求 1 中的上述参数可以包括在非接入层(non access stratum, NAS)消息的容器(container)。这样,一方面,由于中间节点透传 container 不篡改 container 中内容,因此可以保证终端设备 1 的安全能力的安全性;另一方面,由于 AMF1 网元可以不解析上述参数,因此可以节省 AMF1 网元的处理资源,以及提高 AMF1 网元的处理效率。

10 需要说明的是,本申请实施例中,即使上述参数可以包括在 container 中,在 container 之外总会包括终端设备 1 的 3GPP 身份信息。比如,终端设备 1 在向 AMF1 网元发送发现请求 1 时,将终端设备 1 的 3GPP 身份信息包括在 container 中,在 container 之外也包括终端设备 1 的 3GPP 身份信息。在此统一说明,以下不再赘述。

15 可选的,本申请实施例中的发现请求 1 还可以包括终端设备 1 的安全能力。其中,安全能力的相关描述可参考具体实施方式前序介绍部分,在此不再赘述。

一种可能的实现方式中,终端设备 1 的安全能力可以包括在 NAS 消息的容器中。这样,一方面,由于中间节点透传 container 不篡改 container 中内容,因此可以保证终端设备 1 的安全能力的安全性;另一方面,由于 AMF1 网元不需要解析第一设备的安全能力,因此可以节省 AMF1 网元的处理资源,以及提高 AMF1 网元的处理效率。

20 另一种可能的实现方式中,终端设备 1 的安全能力可以包括在 NAS 消息的容器之外。这样,在 AMF1 网元需要获取终端设备 1 的安全能力的情况下,可以直接从 NAS 消息的容器之外获取终端设备 1 的安全能力,节省了 AMF1 网元从终端设备 1 安全上下文获取第一设备的安全能力的步骤,从而可以提高 AMF1 网元的处理效率。

25 可选的,本申请实施例中的发现请求 1 还可以包括终端设备 1 的安全策略。其中,安全策略的相关描述可参考具体实施方式前序介绍部分,在此不再赘述。

一种可能的实现方式中,终端设备 1 的安全策略可以包括在 NAS 消息的容器中。这样,一方面,由于中间节点透传 container 不篡改 container 中内容,因此可以保证终端设备 1 的安全策略的安全性;另一方面,由于 AMF1 网元不需要解析第一设备的安全策略,因此可以简化 AMF1 网元的处理逻辑。

30 可选的,本申请实施例中的终端设备 1 例如可以为 Model A 中的 announcing UE 或者 Model B 中的 discoveree UE;对应的,下述的终端设备 2 可以为 Model A 中的 monitoring UE 或者 Model B 中的 discoverer UE,在此统一说明,以下不再赘述。

S402、AMF1 网元向 DDNMF1 网元发送发现请求 2。相应的,DDNMF1 网元接收来自 AMF1 网元的发现请求 2。其中,发现请求 2 包括终端设备 1 的签约永久标识

35 (subscription permanent identifier, SUPI)、用于 ProSe 业务的身份信息(user identity)、发现模式、发现命令、发现类型和应用标识(application ID)中的一个或多个。

需要说明的是,本申请实施例中,发现请求 2 中包括的用于 ProSe 业务的身份信息(user identity)、发现模式、发现命令、发现类型和应用标识(application ID)等参数是从发现请求 1 中获取的,具体可参考现有技术,在此不再赘述。

本申请实施例中，发现请求 2 中包括的终端设备 1 的 SUPI 是根据发现请求 1 中的终端设备 1 的 3GPP 身份信息转化得到的，具体的转换方法可参考现有技术，在此不再赘述。

可选的，本申请实施例中的发现请求 2 中的上述参数可以包括在 NAS 消息的容器
5 (container) 中，以使得中间节点透传 container 不篡改 container 中内容。

此外，本申请实施例中，发现请求 2 中还包括终端设备 1 的安全能力。

一种可能的实现方式中，本申请实施例中，发现请求 2 中包括的终端设备 1 的安全能力是从发现请求 1 中获取的。即，AMF1 网元转发终端设备 1 的安全能力。该实现方式对应下述场景 1 和场景 2:

10 场景 1、标准规定终端设备 1 的安全能力由终端设备 1 上报（即发现请求 1 中包括终端设备 1 的安全能力），并且终端设备 1 的安全能力包含在 NAS 消息的 container 中，此时 AMF1 网元无需确定发现请求 1 中是否包括终端设备 1 的安全能力，而是直接转发发现请求 1 中包括的终端设备 1 的安全能力。该方案由于不需要 AMF1 网元检查是否携带安全能力，因此能够简化 AMF1 网元的处理逻辑。

15 场景 2、协议未规定终端设备 1 的安全能力必须由终端设备 1 上报，此时 AMF1 网元获取发现请求 1 之后，确定发现请求 1 中是否包括终端设备 1 的安全能力，比如检查 NAS 消息的 container 之外是否包括终端设备 1 的安全能力。若 AMF1 网元确定发现请求 1 中包括终端设备 1 的安全能力，AMF1 网元转发终端设备 1 的安全能力。该方案由于不限定终端设备 1 的安全能力必须由终端设备 1 上报，因此较为灵活。

20 另一种可能的实现方式中，本申请实施例中，发现请求 2 中包括的终端设备 1 的安全能力是 AMF1 网元根据终端设备 1 的 3GPP 身份信息查找 AMF1 网元上存储的终端设备 1 的上下文，从终端设备 1 的上下文中获取到的。该实现方式对应下述场景 3 和场景 4:

25 场景 3、协议未规定终端设备 1 的安全能力必须由终端设备 1 上报，此时 AMF1 网元获取发现请求 1 之后，确定发现请求 1 中是否包括终端设备 1 的安全能力，比如检查 NAS 消息的 container 之外是否包括终端设备 1 的安全能力。若 AMF1 网元确定发现请求 1 中不包括终端设备 1 的安全能力，AMF1 网元根据上述方式获取终端设备 1 的安全能力，并将该终端设备 1 的安全能力包含在 NAS 消息的 container 之外发送给 DDNMF1 网元。该方案由于不限定终端设备 1 的安全能力必须由终端设备 1 上报，因此较为灵活。
30

场景 4、协议未规定终端设备 1 的安全能力必须由终端设备 1 上报，此时 AMF1 网元获取发现请求 1 之后，无需确定发现请求 1 中是否包括终端设备 1 的安全能力，而是直接根据上述方式获取终端设备 1 的安全能力，并将该终端设备 1 的安全能力包含在 NAS 消息的 container 之外发送给 DDNMF1 网元。一方面，由于该方案中终端设备 1 的安全能力是从网络侧获取的，因此能够使得 DDNMF1 网元获得的终端设备 1
35 的安全能力更为准确；另一方面，该方案由于不需要 AMF1 网元检查是否携带安全能力，因此能够简化 AMF1 网元的处理逻辑。

可选的，本申请实施例中，当发现请求 1 中包括终端设备 1 的安全策略时，AMF1 网元还转发终端设备 1 的安全策略，即相应的，发现请求 2 中包括终端设备 1 的安全

策略，在此统一说明，以下不再赘述。

上述步骤 S401-S402 以终端设备 1 通过控制面流程接入 DDNMF1 网元为例进行说明。可选的，本申请实施例中，终端设备 1 也可以通过用户面接入 DDNMF1 网元，本申请实施例对此不做具体限定。其中，终端设备 1 在通过用户面向 DDNMF1 网元发送发现请求的过程中，上述发现请求 1 与发现请求 2 为同一请求消息，终端设备 1 的 3GPP 身份信息可能经过 NEF 网元或者其他网元的“翻译”转化为终端设备 1 的 SUPI；或者，若 DDNMF1 网元获取到的终端设备 1 的 3GPP 身份信息中不包括 SUPI，DDNMF1 网元还可以通过与对应的 UDM1 网元（图中未示出）的交互获取终端设备 1 的 SUPI。示例性的，DDNMF1 网元向 UDM1 网元发送 UE ID 请求（UE ID request）消息，该 UE ID 请求消息包括终端设备 1 的 3GPP 身份信息（比如 GPSI 或 PEI）。UDM1 网元接收来自 DDNMF1 网元的 UE ID 请求消息，并根据终端设备 1 的 3GPP 身份信息（比如 SUCI）确定终端设备 1 的 SUPI 之后，向 DDNMF1 网元发送终端设备 1 的 SUPI。

可选的，本申请实施例中，若终端设备 1 通过用户面接入 DDNMF1 网元，在终端设备 1 发送的发现请求不包括终端设备 1 的安全能力的情况下，DDNMF1 网元可以使用终端设备 1 的 3GPP 身份信息与 AMF1 网元交互以获取终端设备 1 的安全能力，本申请实施例对此不做具体限定。

可选的，本申请实施例中，若终端设备 1 通过控制面流程接入 DDNMF1 网元，则可以使用 SUCI 或者 5G-GUTI 等身份信息作为终端设备 1 的 3GPP 身份信息；若终端设备 1 通过用户面流程接入 DDNMF1 网元，则可以使用 GPSI 或 PEI 等身份信息作为终端设备 1 的 3GPP 身份信息，在此统一说明，以下不再赘述。

可选的，本申请实施例中的发现请求（包括上述发现请求 1 和发现请求 2）中可以包括一个或多个用于 ProSe 业务的 user identity，即终端设备 1 可以同时请求多个 ProSe 业务发现授权和对应的发现参数，本申请实施例对此不做具体限定。

S403、DDNMF1 网元根据终端设备 1 发送的用于 ProSe 业务的 user identity 和/或应用标识对终端设备 1 进行 ProSe 发现授权检查。

可选的，本申请实施例中，DDNMF1 网元可以根据应用标识确定对应的临近业务应用服务器（ProSe app server）并由 ProSe app server 完成授权检查后通知给 DDNMF1 网元。本申请实施例中，ProSe app server 授权检查用于验证终端设备 1 是否可以合法使用该 ProSe 业务，在此统一说明，以下不再赘述。

可选的，本申请实施例中，若终端设备 1 携带了多个用于 ProSe 业务的 user identity，则根据上面的描述，DDNMF1 网元要根据各个用于 ProSe 业务的 user identity，分别对终端设备 1 进行 ProSe 业务发现授权检查，上述多个授权可分别在独立流程中进行，也可在统一的流程中进行，在此统一说明，以下不再赘述。

S404、在 ProSe 业务发现授权检查通过后，DDNMF1 网元获取终端设备 1 的安全策略和发现参数。

本申请实施例中，终端设备 1 获取终端设备 1 的安全策略的方式包括：从发现请求 2 中获取，和/或，根据终端设备 1 的 SUPI 从终端设备 1 对应的 PCF 网元 1（也可以是其他网元）获取。

下面分两种场景讨论安全策略的获取方式：

场景一, DDNMF1 网元确定上述发现请求 2 中未包括终端设备 1 的安全策略, 则:

DDNMF1 网元可以根据终端设备 1 的 SUPI 从终端设备 1 对应的第一 PCF 网元(也可以是其他网元)获取终端设备 1 的安全策略, 该安全策略可以包括一种或多种保护策略, 具体可参考具体实施方式前序部分, 在此不再赘述。

5 场景二, DDNMF1 网元确定上述发现请求 2 中包括终端设备 1 的安全策略, 则:

一种可能的实现方式中, 若上述发现请求 2 中终端设备 1 的安全策略包括 PC5 连接中的用户面机密性保护策略和完整性保护策略, 则 DDNMF1 网元可以从发现请求 2 中获取 PC5 连接中的用户面机密性保护策略和完整性保护策略。相应的, DDNMF1 网元获取的终端设备 1 的安全策略包括: PC5 连接中的用户面机密性保护策略和完整性保护策略。该方案由于 DDNMF1 网元不需要向其他网元获取终端设备 1 的安全策略, 因此能够简化 DDNMF1 网元的处理逻辑。

另一种可能的实现方式中, 若上述发现请求 2 中终端设备 1 的安全策略包括 PC5 连接中的用户面机密性保护策略和完整性保护策略, 则 DDNMF1 网元可以从发现请求 2 中获取 PC5 连接中的用户面机密性保护策略和完整性保护策略, 以及根据终端设备 1 的 SUPI 从终端设备 1 对应的 PCF1 网元(也可以是其他网元)获取 PC5 连接中的控制面机密性保护策略和/或完整性保护策略。相应的, DDNMF1 网元获取的终端设备 1 的安全策略包括: PC5 连接中的用户面机密性保护策略和完整性保护策略、以及 PC5 连接中的控制面机密性保护策略和/或完整性保护策略。该方案由于不限定终端设备 1 必需上报 PC5 连接中的控制面安全策略, 因此较为灵活。

20 需要说明的是, 场景二仅是示例性的提供了两种可能的实现方式。当然, 如具体实施方式前序部分所述, 本申请实施例中的安全策略可以包括至少一种保护策略。在 DDNMF1 网元确定上述发现请求 2 中包括至少一种保护策略时, DDNMF1 网元可以仅从发现请求 2 中获取至少一种保护策略, 即 DDNMF1 网元获取的终端设备 1 的安全策略包括发现请求 2 中携带的至少一种保护策略; 或者, DDNMF1 网元可以从发现请求 2 中获取至少一种保护策略, 并且根据终端设备 1 的 SUPI 从终端设备 1 对应的第一 PCF 网元(也可以是其他网元)获取发现请求 2 中未包含的一种或多种保护策略, 即 DDNMF1 网元获取的终端设备 1 的安全策略包括发现请求 2 中携带的至少一种保护策略、以及从终端设备 1 对应的 PCF 网元 1(也可以是其他网元)获取的发现请求 2 中未包含的一种或多种保护策略。本申请实施例对 DDNMF1 网元获取终端设备 1 的安全策略的方式不做具体限定。

30 可选的, 本申请实施例中, 对于场景二, 即发现请求 2 中包括终端设备 1 的安全策略的场景下, DDNMF1 网元也可以忽略发现请求 2 中包括的终端设备 1 的安全策略, 而是根据终端设备 1 的 SUPI 从终端设备 1 对应的 PCF 网元 1(也可以是其他网元)获取终端设备 1 的安全策略, 本申请实施例对此不作具体限定。一方面, 由于该方案中终端设备 1 的安全策略是从网络侧同步获取的, 因此能够使得 DDNMF1 网元获得的终端设备 1 的安全策略更为准确; 另一方面, 该方案由于不需要 DDNMF1 网元检查是否携带安全策略, 因此能够简化 DDNMF1 网元的处理逻辑。

本申请实施例中, 终端设备 1 的发现参数例如可以如表一所示:

表一

	Model A	Model B
ProSe 发现使用的 code	Prose Restricted Code	ProSe Response Code
发现参数 container	Code-Send-SecParams	Code-Send-SecParams Code-Rcv-SecParams
发现时间限制参数	CURRENT_TIME, MAX_OFFSET	

其中，在 Model A 模式下，Code-Send-SecParams 包含用来在 PC5 接口上的发现流程中保护 Prose Restricted Code 所用的发现参数；在 Model B 模式下，Code-Send-SecParams 用来在 PC5 接口上的发现流程中保护 ProSe Response Code 所用的发现参数，Code-Rcv-SecParams 包含用来在 PC5 接口上的发现流程中获取对端发来的 ProSe 发现使用的 code 所用的发现参数。表一中发现参数的相关描述可参考现有的 3GPP TS 23.303, v15.1.0 和 3GPP TS 33.303, v15.0.0 标准，在此不予赘述。

需要说明的是，本申请实施例以 restricted discovery 的发现场景为例进行说明。在 open discovery 的发现场景下，终端设备 1 的发现参数与表一不同，具体如表二所示：

表二

	Model A
ProSe 发现使用的 code	ProSe Application Code
发现参数	Discovery Key
发现时间限制参数	CURRENT_TIME, MAX_OFFSET

其中，Discovery Key 包含用来在发现流程中保护 ProSe Application Code 所用的发现参数，即上述发现参数用于在 PC5 接口上保护 ProSe 发现使用的 Code。表二中发现参数的相关描述可参考现有的 3GPP TS 23.303, v15.1.0 和 3GPP TS 33.303, v15.0.0 标准，在此不予赘述。

S405、DDNMF1 网元通过 AMF1 网元向终端设备 1 发送发现响应（discovery response）1。相应的，终端设备 1 通过 AMF1 网元接收来自 DDNMF1 网元的发现响应 1。

其中，该发现响应 1 包括 ProSe 发现使用的 code、终端设备 1 的发现参数 container、发现时间限制参数。

可选的，本申请实施例中的发现响应 1 还可以包括终端设备 1 的安全能力。终端设备 1 获取终端设备 1 的安全能力之后，可以存储终端设备 1 的安全能力。一种可能的实现方式中，终端设备 1 存储终端设备 1 的安全能力，包括：终端设备 1 确定终端设备 1 上是否已经存储终端设备 1 的安全能力，若未存储，终端设备 1 存储终端设备 1 的安全能力；若已经存储，终端设备 1 使用发现响应 1 中的安全能力更新已经存储的终端设备 1 的安全能力。

进一步的，可选的，本申请实施例中，在 DDNMF1 网元向终端设备 1 发送终端设备 1 的安全能力之前，DDNMF1 网元可以检查发现请求 2 中包括的终端设备 1 的安全能力是否与 DDNMF1 网元上存储的终端设备 1 的安全能力相同，若不相同或者 DDNMF1 网元上未存储终端设备 1 的安全能力，则 DDNMF1 网元向终端设备 1 发送终端设备 1 的安全能力；否则，DDNMF1 网元可以不需要向终端设备 1 发送终端设备

1 的安全能力，这样可以避免不必要的信令资源浪费。

可选的，本申请实施例中的发现响应 1 还可以包括 DDNMF1 网元获取的终端设备 1 的安全策略。终端设备 1 获取终端设备 1 的安全策略之后，可以存储终端设备 1 的安全策略。一种可能的实现方式中，终端设备 1 存储终端设备 1 的安全策略，包括：

5 终端设备 1 确定终端设备 1 上是否已经存储终端设备 1 的安全策略，若未存储，终端设备 1 存储终端设备 1 的安全策略；若已经存储，终端设备 1 使用发现响应 1 中的安全策略更新已经存储的终端设备 1 的安全策略。

进一步的，可选的，本申请实施例中，对应步骤 S404 中的场景二（即 DDNMF1 网元确定上述发现请求 2 中包括终端设备 1 的安全策略），若标准不限定 DDNMF1 网元仅可以从发现请求 2 获取终端设备 1 的安全策略，则在 DDNMF1 网元向终端设备 1 发送终端设备 1 的安全策略之前，DDNMF1 网元可以确定获取的终端设备 1 的安全策略是否与发现请求 2 中的终端设备 1 的安全策略相同。若不相同，则 DDNMF1 网元向终端设备 1 发送终端设备 1 的安全策略；否则，DDNMF1 网元可以不需要向终端设备 1 发送终端设备 1 的安全策略。这样可以避免不必要的信令资源浪费。当然，若标准规定 DDNMF1 网元仅可以从发现请求 2 获取终端设备 1 的安全策略，则本申请实施例中的发现响应 2 中不需要包括终端设备 1 的安全策略，在此统一说明，以下不再赘述。

可选的，本申请实施例中，终端设备 1 也可以通过用户面从 DDNMF1 网元获取发现响应 1，本申请实施例对此不做具体限定。

20 其中，上述步骤 S401-S404 为终端设备 1 的发现参数、安全策略与安全能力的获取流程，下面将通过步骤 S406-S409 给出终端设备 2 的发现参数、安全策略与安全能力的获取流程。

25 S406、终端设备 2 向 AMF2 网元发送发现请求 3。相应的，AMF2 网元接收来自终端设备 2 的发现请求 3。其中，该发现请求 3 包括终端设备 2 的 3GPP 身份信息、用于 ProSe 业务的身份信息（user identity）、发现模式、发现命令，发现类型和应用标识（application ID）中的一个或多个。

30 S407、AMF2 网元向 DDNMF2 网元发送发现请求 4。相应的，DDNMF2 网元接收来自 AMF2 网元的发现请求 4。其中，发现请求 2 包括终端设备 2 的 SUPI、用于 ProSe 业务的 user identity、发现模式、发现命令、发现类型和应用标识中的一个或多个。此外，本申请实施例中，发现请求 4 中还包括终端设备 2 的安全能力。

S408、DDNMF2 网元根据终端设备 2 发送的用于 ProSe 业务的 user identity 和/或应用标识对终端设备 2 进行 ProSe 发现授权检查。

S409、在 ProSe 业务发现授权检查通过后，DDNMF2 网元获取终端设备 2 的安全策略和发现参数。

35 本申请实施例中，终端设备 2 的发现参数例如可以如表三所示：

表三

	Model A	Model B
ProSe 发现使用的 code	Prose Restricted Code	ProSe Query Code

发现参数 container	Code-Rcv-SecParams	Code-Send-SecParams Code-Rcv-SecParams
发现时间限制参数	CURRENT_TIME, MAX_OFFSET	

其中，在 Model A 模式下，Code-Rcv-SecParams 包含用来在 PC5 接口上的发现流程中保护 ProSe Restricted Code 所用的发现参数；在 Model B 模式下，Code-Send-SecParams 包含用来在 PC5 接口上的发现流程中保护 ProSe Query Code 所用的发现参数，Code-Rcv-SecParams 包含用来在 PC5 接口上的发现流程中获取对端发来的 ProSe 发现使用的 code 所用的发现参数。即上述发现参数用于在 PC5 接口上保护 ProSe 发现使用的 Code。表三中发现参数的相关描述可参考现有的 3GPP TS 23.303，v15.1.0 和 3GPP TS 33.303，v15.0.0 标准，在此不予赘述。

需要说明的是，本申请实施例以 restricted discovery 的发现场景为例进行说明。在 open discovery 的发现场景下，终端设备 2 的发现参数与表三不同，具体如表四所示：

表四

	Model A
ProSe 发现使用的 code	ProSe Application Code
发现时间限制参数	CURRENT_TIME, MAX_OFFSET

需要说明的是，open discovery 的发现场景下，终端设备 2 不需要对应的 discovery key，解密依靠匹配上报（match report）流程。也就是说，此时终端设备 2 不存在对应的发现参数。相关描述可参考现有的 3GPP TS 23.303，v15.1.0 和 3GPP TS 33.303，v15.0.0 标准，在此不予赘述。

其中，上述步骤 S406-S409 的具体实现可参考上述步骤 S401-S404，区别比如在于：将步骤 S401-S404 中的终端设备 1 替换为步骤 S406-S409 中的终端设备 2；将步骤 S401-S404 中的 DDNMF1 网元替换为步骤 S406-S409 中的 DDNMF2 网元；将步骤 S401-S404 中的 AMF1 网元替换为步骤 S406-S409 的 AMF2 网元；将步骤 S401-S404 中的 UDM1 网元替换为步骤 S406-S409 的 UDM2 网元；将步骤 S401-S404 中的 PCF1 网元替换为步骤 S406-S409 的 PCF2 网元等；将步骤 S401-S404 中的发现请求 1 替换为步骤 S406-S409 的发现请求 3，将步骤 S401-S404 中的发现请求 2 替换为步骤 S406-S409 的发现请求 4 等，在此不再详细阐述。此外，需要说明的是，在上述步骤 S406-S409 中，DDNMF2 网元对终端设备 2 进行 ProSe 业务发现授权检查时，临近业务应用服务器可以根据终端设备 2 发送的用于 ProSe 业务的 user identity 确定同样 ProSe 业务的终端设备发送的用于 ProSe 业务的 user identity，并发送给终端设备 2，以便于后续终端设备 2 进行其他的发现，本申请实施例对此不做具体限定。

此外，本申请实施例中，在 DDNMF2 网元对终端设备 2 进行 ProSe 业务发现授权检查的过程中，DDNMF2 网元还可以获取终端设备 1 对应的用于 ProSe 业务的 user identity，具体可参考现有技术，在此不予赘述。

S410、DDNMF2 网元从 DDNMF1 网元获取终端设备 1 的安全参数，该安全参数为建立终端设备 1 与终端设备 2 之间的 PC5 连接所需的安全参数。本申请实施例中的安全参数包括安全策略，和/或安全能力，在此统一说明，以下不再赘述。

本申请实施例中，DDNMF2 网元可以根据步骤 S409 中获取的终端设备 1 对应的

用于 ProSe 业务的 user identity 确定 DDNMF1 网元。

一种可能的实现方式中，本申请实施例中，DDNMF2 网元从 DDNMF1 网元获取终端设备 1 的安全策略，包括：DDNMF2 网元向 DDNMF1 网元发送请求消息，该请求消息包括终端设备 2 发送的用于 ProSe 业务的 user identity、应用标识和终端设备 1 发送的用于 ProSe 业务的 user identity，用于向 DDNMF1 网元请求终端设备 1 的安全参数。DDNMF1 网元接收该请求消息之后，可以向 DDNMF2 网元发送相应的响应消息，该响应消息包括终端设备 1 的安全参数。

S411、DDNMF2 网元根据终端设备 1 的安全参数和终端设备 2 的安全参数是否匹配，确定终端设备 1 与终端设备 2 是否支持互相通信。

本申请实施例中，DDNMF2 网元根据终端设备 1 的安全参数和终端设备 2 的安全参数是否匹配，确定终端设备 1 与终端设备 2 是否支持互相通信，包括：

当终端设备 1 的安全参数和终端设备 2 的安全参数不匹配时，DDNMF2 网元确定终端设备 1 和终端设备 2 不支持互相通信；或者，当终端设备 1 的安全参数和终端设备 2 的安全参数匹配时，DDNMF2 网元确定终端设备 1 和终端设备 2 支持互相通信。

一种可能的实现方式中，本申请实施例中的安全信息包括安全策略。终端设备 1 的安全参数和终端设备 2 的安全参数匹配是指，终端设备 1 的安全策略与终端设备 2 的安全策略匹配。终端设备 1 的安全参数和终端设备 2 的安全参数不匹配是指，终端设备 1 的安全策略与终端设备 2 的安全策略不匹配。

一种可能的实现方式中，本申请实施例中的安全信息包括安全能力。终端设备 1 的安全参数和终端设备 2 的安全参数匹配是指，终端设备 1 的安全能力与终端设备 2 的安全能力匹配。终端设备 1 的安全参数和终端设备 2 的安全参数不匹配是指，终端设备 1 的安全能力与终端设备 2 的安全能力不匹配。

一种可能的实现方式中，本申请实施例中的安全信息包括安全能力和安全策略。终端设备 1 的安全参数和终端设备 2 的安全参数匹配是指，终端设备 1 的安全能力与终端设备 2 的安全能力匹配，并且终端设备 1 的安全策略与终端设备 2 的安全策略匹配，否则认为终端设备 1 的安全参数和终端设备 2 的安全参数不匹配。

其中，安全能力是否匹配、或者安全策略是否匹配的相关描述可参考具体实施方式前序部分，在此不再赘述。

进一步的，本申请实施例中，若 DDNMF2 网元确定终端设备 1 与终端设备 2 不支持互相通信，则执行步骤 S412，否则执行步骤 S413。

S412、DDNMF2 网元通过 AMF2 网元向终端设备 2 发送指示信息 1。相应的，终端设备 2 通过 AMF2 网元接收来自 DDNMF2 网元的指示信息 1。指示信息 1 用于指示终端设备 1 与终端设备 2 之间不支持互相通信。

S413、DDNMF2 网元通过 AMF2 网元向终端设备 2 发送发现响应 2。相应的，终端设备 2 通过 AMF2 网元接收来自 DDNMF2 网元的发现响应 2。

其中，该发现响应 2 包括 ProSe 发现使用的 code、终端设备 2 的发现参数、发现时间限制参数。

可选的，本申请实施例中的发现响应 2 还可以包括终端设备 2 的安全能力。终端设备 2 获取终端设备 2 的安全能力之后，可以存储终端设备 2 的安全能力。一种可能

的实现方式中,终端设备2存储终端设备2的安全能力,包括:终端设备2确定终端设备2上是否已经存储终端设备2的安全能力,若未存储,终端设备2存储终端设备2的安全能力;若已经存储,终端设备2使用发现响应2中的安全能力更新已经存储的终端设备1的安全能力。

- 5 进一步的,可选的,本申请实施例中,在DDNMF2网元向终端设备2发送终端设备1的安全能力之前,DDNMF2网元可以检查发现请求4中包括的终端设备2的安全能力是否与DDNMF2网元上存储的终端设备2的安全能力相同,若不相同或者DDNMF2网元上未存储终端设备2的安全能力,则DDNMF2网元向终端设备2发送终端设备2的安全能力;否则,DDNMF2网元可以不需要向终端设备2发送第人终端设备的
10 安全能力,这样可以避免不必要的信令资源浪费。

- 可选的,本申请实施例中的发现响应2还可以包括DDNMF2网元获取的终端设备2的安全策略。终端设备2获取终端设备2的安全策略之后,可以存储终端设备2的安全策略。一种可能的实现方式中,终端设备2存储终端设备2的安全策略,包括:终端设备2确定终端设备2上是否已经存储终端设备2的安全策略,若未存储,终端
15 设备2存储终端设备2的安全策略;若已经存储,终端设备2使用发现响应2中的安全策略更新已经存储的终端设备2的安全策略。

- 进一步的,可选的,本申请实施例中,在DDNMF2网元确定上述发现请求4中包括终端设备2的安全策略的场景下,若标准未规定DDNMF2网元仅可以从发现请求4获取终端设备2的安全策略,则在DDNMF2网元向终端设备2发送终端设备2的安全
20 策略之前,DDNMF2网元可以确定获取的终端设备2的安全策略是否与发现请求4中的终端设备2的安全策略相同。若不相同,则DDNMF2网元向终端设备2发送终端设备2的安全策略;否则,DDNMF2网元可以不需要向终端设备2发送第人终端设备的安全策略。这样可以避免不必要的信令资源浪费。当然,若标准规定DDNMF2网元仅可以从发现请求4获取终端设备2的安全策略,则本申请实施例中的发现响应2中不
25 需要包括终端设备2的安全策略,在此统一说明,以下不再赘述。

可选的,本申请实施例中,终端设备2也可以通过用户面从DDNMF2网元获取发现响应2,本申请实施例对此不做具体限定。

- 需要说明的是,上述步骤S410-411以DDNMF2网元确定终端设备1与终端设备2是否支持互相通信为例进行说明。可选的,本申请实施例中,也可以由DDNMF1网元从DDNMF2网元获取终端设备1的安全参数,该安全参数为建立终端设备1与终端
30 设备2之间的PC5连接所需的安全参数,进而DDNMF1网元根据终端设备1的安全参数和终端设备2的安全参数是否匹配,确定终端设备1与终端设备2是否支持互相通信,实现方式与上述步骤S410-S411类似,在此不再赘述。

- 进一步的,若DDNMF1网元确定终端设备1与终端设备2不支持互相通信,
35 DDNMF1网元可以向DDNMF2网元发送指示信息2,该指示信息2用于指示终端设备1与终端设备2不支持互相通信,进而DDNMF2网元继续执行上述步骤S412。

或者,若DDNMF1网元确定终端设备1与终端设备2支持互相通信,一种可能的实现方式中,DDNMF1网元向DDNMF2网元发送终端设备1的发现参数,该发现参数用于隐式指示终端设备1与终端设备2支持互相通信,DDNMF2网元获取终端设备

1 的发现参数后，继续执行上述步骤 S413。另一种可能的实现方式中，DDNMF1 网元向 DDNMF2 网元发送终端设备 1 的发现参数和指示信息 3，该指示信息 3 用于指示终端设备 1 与终端设备 2 支持互相通信。DDNMF2 网元根据指示信息 3，继续执行上述步骤 S413，本申请实施例对此不做具体限定。

5 可选的，本申请实施例中，若 DDNMF2 网元确定终端设备 1 与终端设备 2 支持互相通信，则进一步的，可以由 DDNMF2 网元确定终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法。进而，第二 DDNMF 可以将选定的安全保护方法和使用的安全保护算法发送给 DDNMF1 网元，由 DDNMF1 网元将选定的安全保护方法和使用的安全保护算法发送给终端设备 1。若 DDNMF1 网元确定终端设备
10 1 与终端设备 2 支持互相通信，则进一步的可由 DDNMF1 网元确定终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法，并由 DDNMF1 网元将选定的安全保护方法和使用的安全保护算法发送给终端设备 1，本申请实施例对此不作具体限定。

可选的，本申请实施例中，若 DDNMF2 网元确定终端设备 1 与终端设备 2 支持互
15 相通信，则进一步的，可以由 DDNMF2 网元确定终端设备 1 与终端设备 2 之间 PC5 连接的安全保护和使用的安全保护算法。进而，第二 DDNMF 可以将选定的安全保护方法和使用的安全保护算法发送给终端设备 2(比如通过上述发现响应 2)。若 DDNMF1 网元确定终端设备 1 与终端设备 2 支持互相通信，则进一步的可由 DDNMF1 网元确定终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法，并由
20 DDNMF1 网元将选定的安全保护方法和使用的安全保护算法发送给 DDNMF2 网元，由 DDNMF2 网元将选定的安全保护方法和使用的安全保护算法发送给终端设备 2，本申请实施例对此不作具体限定。

进一步的，本申请实施例中，在步骤 S413 之后，还可以发现广播流程。

以 Model A 发现场景为例，则本申请实施例提供的通信方法还可以包括如下步骤
25 骤 S414-S415：

S414、终端设备 1 向终端设备 2 发送广播 (announcing) 消息。相应的，终端设备 2 接收来自终端设备 1 的广播消息。

可选的，本申请实施例中的广播消息可以包括终端设备 1 的安全参数，终端设备 1 的安全参数用于进一步辅助终端设备 2 确定是否可以建立后续通信，本申请实施例
30 对此不做具体限定。

一种可能的实现方式中，本申请实施例中的广播消息的保护方法可以遵循现有技术中的发现参数指示，具体可参考现有技术，在此不再赘述。

另一种可能的实现方式中，如果终端设备 1 获取到终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法，则本申请实施例中的广播消息的保护方法可以采用该安全保护方法和安全保护算法。例如，终端设备 1 与终端设备 2 之
35 间 PC5 连接的安全保护方法为控制面完整性保护开启，使用完整性保护算法 NIA1，则可以对该广播消息使用 NIA1 进行完整性保护。

S415、终端设备 2 验证广播消息。

步骤 S415 可参考现有的实现方式，在此不再赘述。

可选的，本申请实施例中，终端设备 2 验证广播消息准确后，还可以继续验证终端设备 1 的安全参数与终端设备 2 的安全参数是否匹配，如匹配继续进行后续通信，如不匹配则断开连接，本申请实施例对此不做具体限定。

以 Model B 发现场景为例，则本申请实施例提供的通信方法还可以包括如下步骤 5 骤 S416-S419:

S416、终端设备 2 向终端设备 1 发送请求代码 (send query code) 消息。相应的，终端设备 1 接收来自终端设备 2 的发送请求代码消息。

可选的，本申请实施例中的发送请求代码消息可以包括终端设备 1 的安全参数，终端设备 1 的安全参数用于进一步辅助终端设备 2 确定是否可以建立后续通信，本申请实施例对此不做具体限定。

一种可能的实现方式中，本申请实施例中的发送请求代码消息的保护方法可以遵循现有技术中的发现参数指示，具体可参考现有技术，在此不再赘述。

另一种可能的实现方式中，如果终端设备 2 获取到终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法，则本申请实施例中的发送请求代码消息的保护方法可以采用该安全保护方法和安全保护算法。例如，终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法为控制面完整性保护开启，使用完整性保护算法 NIA2，则可以对该发送请求代码消息使用 NIA2 进行完整性保护。

S417、终端设备 1 验证发送请求代码消息。

步骤 S417 可参考现有的实现方式，在此不再赘述。

可选的，本申请实施例中，终端设备 1 验证发送请求代码消息准确后，还可以继续验证终端设备 1 的安全参数与终端设备 2 的安全参数是否匹配，如匹配继续进行后续通信，如不匹配则断开连接，本申请实施例对此不做具体限定。

可选的，本申请实施例中，若终端设备 2 提供了终端设备 2 的安全参数，则终端设备 2 可以确定终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法，本申请实施例对此不做具体限定。

S418、终端设备 1 向终端设备 2 发送响应代码 (Send response Code) 消息。相应的，终端设备 2 接收来自终端设备 1 的发送响应代码消息。

可选的，本申请实施例中的响应代码消息可以包括终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法。

一种可能的实现方式中，本申请实施例中的发送响应代码消息的保护方法可以遵循现有技术中的发现参数指示，具体可参考现有技术，在此不再赘述。

另一种可能的实现方式中，如果终端设备 1 获取到终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法，则本申请实施例中的发送响应代码消息的保护方法可以采用该安全保护方法和安全保护算法。例如，终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法为控制面完整性保护开启，使用的完整性保护算法为 NIA3，则可以对该发送响应代码消息使用 NIA1 完整性保护算法进行完整性保护。

S419、终端设备 2 验证发送响应代码消息。

步骤 S419 可参考现有的实现方式，在此不再赘述。

可选的，本申请实施例中，终端设备 2 验证发送响应代码消息准确后，还可以继

续验证自己是否可以满足终端设备 1 提供的 PC5 连接的安全保护方法和使用的安全保护算法,如可以满足则继续建立通信,否则断开连接。

可选的,本申请实施例中,在 Model A 或者 Model B 上述流程结束之后,还可能包括 match report 流程,具体可参考现有的 3GPP TS 23.303, v15.1.0 和 3GPP TS 33.303, v15.0.0 标准,在此不予赘述。

现有的 V2X 场景将安全协商引入 PC5 单播建立流程,两端终端设备的安全参数的不一致将会导致 PC5 单播建立失败。此时由于已经完成 ProSe 发现流程,也执行了 PC5 单播建立流程的部分步骤,因此将造成过多的信令浪费。本申请实施例可以在 ProSe 发现流程中对终端设备 1 的安全参数与终端设备 2 的安全参数进行匹配,并且在终端设备 1 的安全参数和终端设备 2 的安全参数不匹配的情况下,指示终端设备 1 与终端设备 2 不支持互相通信,使得可以及时终止终端设备 1 与终端设备 2 之间的 ProSe 发现流程,因此可以避免现有技术中在 ProSe 发现流程之后的 PC5 单播建立流程中,两端终端设备的安全参数的不一致导致 PC5 单播建立失败所带来的信令浪费的问题。

其中,上述步骤 S401 至 S419 中 DDNMF1 网元或者 DDNMF2 网元的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该 DDNMF1 网元或者 DDNMF2 网元执行,本实施例对此不作任何限制。

示例性的,本申请实施例提供另一种通信方法,该通信方法以图 2 所示的 5G 网络中 ProSe 控制面架构为例,依赖于 ProSe 发现流程中的 match report 流程,而非在 ProSe 发现流程中的发现参数获取流程中进行安全参数的匹配。此外,本申请实施例的流程适用于 open discovery 和 restricted discovery 两种场景。如图 5 所示,该通信方法包括如下步骤:

S501、ProSe 发现流程中的发现参数获取流程与发现广播流程,具体可参考现有的 4G ProSe 发现流程,在此不再赘述。其中,终端设备 2 在发现参数获取流程中获取终端设备 1 对应的用于 ProSe 业务的 user identity,以及终端设备 2 在发现广播流程中获取终端设备 1 的 3GPP 身份信息和 ProSe 发现使用的 code。

需要说明的是,在 5G 网络中 ProSe Function 中 ProSe 发现相关功能由 5G DDNMF 网元(比如本申请实施例中的 DDNMF1 网元与 DDNMF2 网元)代替,在此统一说明,以下不再赘述。

需要说明的是,本申请实施例中,在 ProSe 发现流程中的发现参数获取流程中,终端设备 2 需要获取后续触发 match report 的指示,在此统一说明,以下不再赘述。

S502、终端设备 2 根据触发 match report 的指示,在发现终端设备 1 之后触发 match report 流程。

可选的,本申请实施例中的终端设备 2 可以为 Model A 中的 monitoring UE 或者 Model B 中的 discoverer UE,本申请实施例中的终端设备 1 例如可以为 Model A 中的 announcing UE 或者 Model B 中的 discoveree UE,在此统一说明,以下不再赘述。

S503、终端设备 2 向 DDNMF2 网元发送 match report 消息。相应的 DDNMF2 网元接收来自终端设备 2 的 match report 消息。其中,该 match report 消息包括终端设备 1 的 3GPP 身份信息、终端设备 2 的 3GPP 身份信息、终端设备 1 对应的用于 ProSe 业

务的 user identity、终端设备 2 对应的用于 ProSe 业务的 user identity、发现模式、发现命令、发现类型和应用标识 (application ID) 中的一个或多个。其中, 终端设备 1 的 3GPP 身份信息、终端设备 2 的 3GPP 身份信息、终端设备 1 对应的用于 ProSe 业务的 user identity、终端设备 2 对应的用于 ProSe 业务的 user identity、发现模式、发现命令、
5 发现类型和应用标识的相关描述可参考图 4 所示的实施例, 在此不再赘述。

可选的, 本申请实施例中, 终端设备 2 可以通过用户面向 DDNMF2 网元发送 match report 消息; 或者, 终端设备 2 可以通过控制面向 DDNMF2 网元发送 match report 消息, 比如, 终端设备 2 使用 NAS 消息将 match report 消息发送至 AMF2 网元后, 由 AMF2 网元转发 NAS 该消息中的 container 和/或参数至 DDNMF2 网元, 本申请实施例
10 对此不作具体限定。其中, match report 消息在终端设备 2 与 DDNMF2 网元之间的传输方式可参考图 1 所示的实施例, 在此不再赘述。

可选的, 本申请实施例中的 match report 消息还可以包括终端设备 2 的安全策略。其中, 安全策略的相关描述可参考具体实施方式前序介绍部分, 在此不再赘述。

可选的, 本申请实施例中的 match report 消息还可以包括终端设备 2 的安全能力。
15 其中, 安全能力的相关描述可参考具体实施方式前序介绍部分, 在此不再赘述。

S504、DDNMF2 网元获取终端设备 2 的安全参数, 该安全参数为建立终端设备 1 与终端设备 2 之间的 PC5 连接所需的安全参数。

其中, 本申请实施例中的安全参数包括安全策略和/或安全能力。

其中, 本申请实施例中, DDNMF2 网元获取终端设备 2 的安全策略的方式与图 4
20 所示的实施例中 DDNMF2 网元获取终端设备 2 的安全策略的方式类似, 区别比如在于, 将图 4 所示的实施例中的发现请求 1 或发现请求 2 替换为本申请实施例中的 match report 消息, 在此不再赘述。

本申请实施例中, DDNMF2 网元获取终端设备 2 的安全能力的方式与图 4 所示的实施例中 DDNMF2 网元获取终端设备 2 的安全能力的方式类似, 区别比如在于, 将图
25 4 所示的实施例中的发现请求或发现请求 2 替换为本申请实施例中的 match report 消息, 在此不再赘述。

S505、DDNMF2 网元确定终端设备 1 对应的 DDNMF1 网元之后, 向 DDNMF1 网元发送终端设备 1 的 3GPP 身份信息和终端设备 2 的安全参数。相应的, DDNMF1 网元接收来自 DDNMF2 网元的终端设备 1 的 3GPP 身份信息和终端设备 2 的安全参数。

30 本申请实施例中, DDNMF2 网元可以根据步骤 S501 中获取的终端设备 1 的 3GPP 身份信息、ProSe 发现使用的 code 或者终端设备 1 对应的用于 ProSe 业务的 user identity 中的一种或几种确定终端设备 1 对应的 DDNMF1 网元。

S506、DDNMF1 网元根据终端设备 1 的 3GPP 身份信息获取终端设备 1 的安全参数。

35 本申请实施例中, DDNMF1 网元获取终端设备 1 的 3GPP 身份信息之后, 可以根据终端设备 1 的 3GPP 身份信息获取终端设备 1 的 SUPI, 具体获取方式与图 4 中 DDNMF1 网元根据终端设备 1 的 3GPP 身份信息获取终端设备 1 的 SUPI 类似, 此处不再赘述。进一步的, DDNMF1 网元获取终端设备 1 的安全策略的方式与图 4 所示的实施例中 DDNMF1 网元根据终端设备 1 的 SUPI 从终端设备 1 对应的 PCF 网元 1 (也

可以是其他网元)获取终端设备1的安全策略的方式相同,在此不再赘述。

本申请实施例中,DDNMF1网元可以使用终端设备1的SUPI与终端设备1对应的AMF1网元交互以获取终端设备1的安全能力,本申请实施例对此不做具体限定。

5 S507、DDNMF1网元根据终端设备1的安全参数和终端设备2的安全参数是否匹配,确定终端设备1与终端设备2是否支持互相通信。

其中,步骤S507的具体实现可参考图4所示的实施例中的步骤S411,区别在于图4所示的实施例步骤S411中,由DDNMF2网元确定终端设备1与终端设备2是否支持互相通信,本申请实施例中,由DDNMF1网元确定终端设备1与终端设备2是否支持互相通信,在此不再赘述。

10 可选的,本申请实施例中,若DDNMF1网元确定终端设备1与终端设备2支持互相通信,DDNMF1网元还可以进一步确定终端设备1与终端设备2之间PC5连接的安全保护方法和使用的安全保护算法。

15 S508、DDNMF1网元向DDNMF2网元发送指示信息4。相应的,DDNMF2网元接收来自DDNMF1网元的指示信息4。其中,指示信息4用于指示终端设备1和终端设备2是否支持互相通信。

20 可选的,本申请实施例中,若DDNMF1网元可以确定终端设备1与终端设备2之间PC5连接的安全保护方法和使用的安全保护算法,则DDNMF1网元还可以向DDNMF2网元发送PC5连接的安全保护方法和使用的安全保护算法。相应的,DDNMF2网元接收来自DDNMF1网元的PC5连接的安全保护方法和使用的安全保护算法。

S509、DDNMF2网元向终端设备2发送match report确认消息。相应的,终端设备2接收来自DDNMF2网元的match report确认消息。其中,该match report确认消息包括指示信息5。指示信息5用于指示终端设备1和终端设备2是否支持互相通信。

25 本申请实施例中,指示信息5可以与指示信息4相同,也可以是指示信息4的变形,本申请实施例对此不做具体限定。

30 可选的,本申请实施例中,若DDNMF2网元可以获取PC5连接的安全保护方法和使用的安全保护算法,则该match report确认消息还可以包括PC5连接的安全保护方法和使用的安全保护算法。这样后续的PC5单播建立流程中,终端设备1与终端设备2之间可以不需要协商PC5连接的安全保护方法和使用的安全保护算法,从而不仅可以节省PC5单播建立流程的信令开销,而且可以降低PC5单播建立流程的实现复杂度。

S510、终端设备2根据指示信息5确定是否支持与终端设备1互相通信。

35 本申请实施例中,若终端设备2根据指示信息5确定支持与终端设备1互相通信,则可以继续后续的PC5单播建立流程;或者,若终端设备2根据指示信息5确定不支持与终端设备1互相通信,则确定不执行后续的PC5单播建立流程。

可选的,本申请实施例提供的通信方法还可以包括步骤S511-S512:

S511、DDNMF1网元向终端设备1发送指示信息6。相应的,终端设备1接收来自DDNMF1网元的指示信息6。其中,指示信息6用于指示终端设备1和终端设备2是否支持互相通信。

本申请实施例中，指示信息 6 可以与指示信息 4 相同，也可以是指示信息 4 的变形，本申请实施例对此不做具体限定。

可选的，本申请实施例中，若 DDNMF1 网元可以确定终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法，则 DDNMF1 网元还可以向终端设备 1 发送 PC5 连接的安全保护方法和使用的安全保护算法。相应的，终端设备 1 接收来自 DDNMF1 网元的 PC5 连接的安全保护方法和使用的安全保护算法。这样后续的 PC5 单播建立流程中，终端设备 1 与终端设备 2 之间可以不需要协商 PC5 连接的安全保护方法和使用的安全保护算法，从而不仅可以节省 PC5 单播建立流程的信令开销，而且可以降低 PC5 单播建立流程的实现复杂度。

10 S512、终端设备 1 根据指示信息 6 确定是否支持与终端设备 2 互相通信。

本申请实施例中，若终端设备 1 根据指示信息 6 确定支持与终端设备 2 互相通信，则可以继续后续的 PC5 单播建立流程；或者，若终端设备 1 根据指示信息 6 确定不支持与终端设备 2 互相通信，则确定不执行后续的 PC5 单播建立流程，进而终端设备 1 可以释放发现广播流程中获取的终端设备 2 的上下文，以降低存储负担。

15 现有的 V2X 场景将安全协商引入 PC5 单播建立流程，两端终端设备的安全参数的不一致将会导致 PC5 单播建立失败。此时由于已经完成 ProSe 发现流程，也执行了 PC5 单播建立流程的部分步骤，因此将造成过多的信令浪费。本申请实施例可以在 ProSe 发现流程中对终端设备 1 的安全参数与终端设备 2 的安全参数进行匹配，并且在终端设备 1 的安全参数和终端设备 2 的安全参数不匹配的情况下，指示终端设备 1 与终端设备 2 不支持互相通信，使得可以及时终止终端设备 1 与终端设备 2 之间的 ProSe 发现流程，因此可以避免现有技术中在 ProSe 发现流程之后的 PC5 单播建立流程中，两端终端设备的安全参数的不一致导致 PC5 单播建立失败所带来的信令浪费的问题。

25 其中，上述步骤 S501 至 S512 中 DDNMF1 网元或者 DDNMF2 网元的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该 DDNMF1 网元或者 DDNMF2 网元执行，本实施例对此不作任何限制。

示例性的，本申请实施例提供另一种通信方法，该通信方法以图 2 所示的 5G 网络中 ProSe 控制面架构为例，依赖于 ProSe 发现流程中的 match report 流程，而非在 ProSe 发现流程中的发现参数获取流程中进行安全参数的匹配。此外，本申请实施例的流程适用于 open discovery 和 restricted discovery 两种场景。如图 6 所示，该通信方法包括如下步骤：

S601-S604、同图 5 所示的实施例中的步骤 S501-S504，相关描述可参考图 5 所示的实施例，在此不再赘述。

35 S605、DDNMF2 网元确定终端设备 1 对应的 DDNMF1 网元之后，向 DDNMF1 网元发送请求消息。相应的，DDNMF1 网元接收来自 DDNMF2 网元的请求消息。该请求消息包括终端设备 1 的 3GPP 身份信息，用于请求终端设备 1 的安全参数。

其中，本申请实施例中，DDNMF2 网元确定 DDNMF1 网元的方式可参考图 5 所示的实施例，在此不再赘述。

S606、DDNMF1 网元根据终端设备 1 的 3GPP 身份信息获取终端设备 1 的安全参

数。

其中，DDNMF1网元根据终端设备1的3GPP身份信息获取终端设备1的安全参数的方式可参考图5所示的实施例，在此不再赘述。

5 S607、DDNMF1网元向DDNMF2网元发送响应消息。相应的，DDNMF2网元接收来自DDNMF1网元的响应消息。该响应消息包括终端设备1的安全参数。

S608、DDNMF2网元根据终端设备1的安全参数和终端设备2的安全参数是否匹配，确定终端设备1与终端设备2是否支持互相通信。

其中，步骤S608的具体实现可参考图4所示的实施例中的步骤S411，在此不再赘述。

10 可选的，本申请实施例中，若DDNMF2网元确定终端设备1与终端设备2支持互相通信，DDNMF2网元还可以进一步确定终端设备1与终端设备2之间PC5连接的安全保护方法和使用的安全保护算法。

15 S609、DDNMF2网元向终端设备2发送match report确认消息。相应的，终端设备2接收来自DDNMF2网元的match report确认消息。其中，该match report确认消息包括指示信息7。指示信息7用于指示终端设备1和终端设备2是否支持互相通信。

可选的，本申请实施例中，若DDNMF2网元可以获取PC5连接的安全保护方法和使用的安全保护算法，则该match report确认消息还可以包括PC5连接的安全保护方法和使用的安全保护算法。这样后续的PC5单播建立流程中，终端设备1与终端设备2之间可以不需要协商PC5连接的安全保护方法和使用的安全保护算法，从而不仅可以节省PC5单播建立流程的信令开销，而且可以降低PC5单播建立流程的实现复杂度。

S610、终端设备2根据指示信息7确定是否支持与终端设备1互相通信。

25 本申请实施例中，若终端设备2根据指示信息7确定支持与终端设备1互相通信，则可以继续后续的PC5单播建立流程；或者，若终端设备2根据指示信息7确定不支持与终端设备1互相通信，则确定不执行后续的PC5单播建立流程。

可选的，本申请实施例提供的通信方法还可以包括如下步骤S611-S613：

S611、DDNMF2网元向DDNMF1网元发送指示信息8。相应的，DDNMF2网元接收来自DDNMF1网元的指示信息8。其中，指示信息8用于指示终端设备1和终端设备2是否支持互相通信。

30 本申请实施例中，指示信息8可以与指示信息7相同，也可以是指示信息7的变形，本申请实施例对此不做具体限定。

可选的，本申请实施例中，若DDNMF2网元可以确定终端设备1与终端设备2之间PC5连接的安全保护方法和使用的安全保护算法，则DDNMF2网元还可以向DDNMF1网元发送PC5连接的安全保护方法和使用的安全保护算法。相应的，
35 DDNMF1网元接收来自DDNMF2网元的PC5连接的安全保护方法和使用的安全保护算法。

S612、DDNMF1网元向终端设备1发送指示信息9。相应的，终端设备1接收来自DDNMF1网元的指示信息9。其中，指示信息9用于指示终端设备1和终端设备2是否支持互相通信。

本申请实施例中，指示信息 9 可以与指示信息 8 相同，也可以是指示信息 8 的变形，本申请实施例对此不做具体限定。

可选的，本申请实施例中，若 DDNMF1 网元可以获取终端设备 1 与终端设备 2 之间 PC5 连接的安全保护方法和使用的安全保护算法，则 DDNMF1 网元还可以向终端设备 1 发送 PC5 连接的安全保护方法和使用的安全保护算法。相应的，终端设备 1 接收来自 DDNMF1 网元的 PC5 连接的安全保护方法和使用的安全保护算法。

S613、终端设备 1 根据指示信息 9 确定是否支持与终端设备 2 互相通信。

本申请实施例中，若终端设备 1 根据指示信息 9 确定支持与终端设备 2 互相通信，则可以继续后续的 PC5 单播建立流程；或者，若终端设备 1 根据指示信息 9 确定不支持与终端设备 2 互相通信，则确定不执行后续的 PC5 单播建立流程，进而终端设备 1 可以释放发现广播流程中获取的终端设备 2 的上下文，以降低存储负担。

现有的 V2X 场景将安全协商引入 PC5 单播建立流程，两端终端设备的安全参数的不一致将会导致 PC5 单播建立失败。此时由于已经完成 ProSe 发现流程，也执行了 PC5 单播建立流程的部分步骤，因此将造成过多的信令浪费。本申请实施例可以在 ProSe 发现流程中对终端设备 1 的安全参数与终端设备 2 的安全参数进行匹配，并且在终端设备 1 的安全参数和终端设备 2 的安全参数不匹配的情况下，指示终端设备 1 与终端设备 2 不支持互相通信，使得可以及时终止终端设备 1 与终端设备 2 之间的 ProSe 发现流程，因此可以避免现有技术中在 ProSe 发现流程之后的 PC5 单播建立流程中，两端终端设备的安全参数的不一致导致 PC5 单播建立失败所带来的信令浪费的问题。

其中，上述步骤 S601 至 S613 中 DDNMF1 网元或者 DDNMF2 网元的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该 DDNMF1 网元或者 DDNMF2 网元执行，本实施例对此不作任何限制。

如图 7 所示，为本申请实施例提供的一种通信方法，包括如下步骤：

S701、第一直连通信发现名称管理功能网元获取第一终端设备的安全参数。该安全参数为建立第一终端设备与第二终端设备之间的 PC5 连接所需的安全参数。

S702、第一直连通信发现名称管理功能网元接收来自第二直连通信发现名称管理功能网元的第二终端设备的安全参数。

S703、第一直连通信发现名称管理功能网元根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信。

对于上述步骤 S701-S703：

第一直连通信发现名称管理功能网元例如可以为图 4 中的 DDNMF1 网元，第一终端设备例如可以为图 4 中的终端设备 1，第二直连通信发现名称管理功能网元例如可以为图 4 中的 DDNMF2 网元，第二终端设备例如可以为图 4 中的终端设备 2；

或者，第一直连通信发现名称管理功能网元例如可以为图 4 中的 DDNMF2 网元，第一终端设备例如可以为图 4 中的终端设备 2，第二直连通信发现名称管理功能网元例如可以为图 4 中的 DDNMF1 网元，第二终端设备例如可以为图 4 中的终端设备 1；

或者，第一直连通信发现名称管理功能网元例如可以为图 5 中的 DDNMF1 网元，第一终端设备例如可以为图 5 中的终端设备 1，第二直连通信发现名称管理功能网元

例如可以为图 5 中的 DDNMF2 网元, 第二终端设备例如可以为图 5 中的终端设备 2;

或者, 第一直连通信发现名称管理功能网元例如可以为图 6 中的 DDNMF2 网元, 第一终端设备例如可以为图 6 中的终端设备 2, 第二直连通信发现名称管理功能网元例如可以为图 6 中的 DDNMF1 网元, 第二终端设备例如可以为图 6 中的终端设备 1。

5 其中, 图 7 所示的实施例的具体实现可参考图 4 至图 6 所示的任一实施例, 在此不再赘述。现有的 V2X 场景将安全协商引入 PC5 单播建立流程, 两端终端设备的安全参数的不一致将会导致 PC5 单播建立失败。此时由于已经完成 ProSe 发现流程, 也执行了 PC5 单播建立流程的部分步骤, 因此将造成过多的信令浪费。本申请实施例可以在 ProSe 发现流程中对第一终端设备的安全参数与第二终端设备的安全参数进行匹
10 配, 并根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配, 确定第一终端设备和第二终端设备是否支持互相通信。进而, 若第一终端设备与第二终端设备不支持互相通信, 可以及时终止当前的 ProSe 发现流程, 因此可以避免现有技术中在 ProSe 发现流程之后的 PC5 单播建立流程中, 两端终端设备的安全参数的不一致导致 PC5 单播建立失败所带来的信令浪费的问题。

15 其中, 上述步骤 S701 至 S703 中第一直连通信发现名称管理功能网元的动作可以由图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的应用程序代码以指令该第一直连通信发现名称管理功能网元执行, 本实施例对此不作任何限制。

可以理解的是, 图 7 所示的实施例中, 由第一直连通信发现名称管理功能网元实现的方法和/或步骤, 也可以由可用于第一直连通信发现名称管理功能网元的部件 (例
20 如芯片或者电路) 实现。

上述主要从各个网元之间交互的角度对本申请实施例提供的方案进行了介绍。相应的, 本申请实施例还提供了通信装置, 该通信装置可以为上述方法实施例中的第一直连通信发现名称管理功能网元, 或者包含上述第一直连通信发现名称管理功能网元的装置, 或者为可用于第一直连通信发现名称管理功能网元的部件。可以理解的是,
25 该通信装置为了实现上述功能, 其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到, 结合本文中所公开的实施例描述的各示例的单元及算法步骤, 本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行, 取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能, 但是这种实现不应认为超出本申请的范围。

图 8 示出了一种通信装置 80 的结构示意图。该通信装置 80 包括收发模块 801 和处理模块 802。所述收发模块 801, 也可以称为收发单元用以实现收发功能, 例如可以是收发电路, 收发机, 收发器或者通信接口。

以通信装置 80 为上述方法实施例中的第一直连通信发现名称管理功能网元或者
35 设置在该第一直连通信发现名称管理功能网元中的芯片或其他部件为例, 一种可能的实现方式中:

处理模块 802, 用于获取第一终端设备的安全参数, 该安全参数为建立第一终端设备与第二终端设备之间的 PC5 连接所需的安全参数。收发模块 801, 用于接收来自第二直连通信发现名称管理功能网元的第二终端设备的安全参数。处理模块 802, 还

用于根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信。

- 5 可选的，处理模块 802，用于根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信，包括：用于当第一终端设备的安全参数和第二终端设备的安全参数不匹配时，确定第一终端设备和第二终端设备不支持互相通信。

可选的，收发模块 801，还用于发送第一指示信息，第一指示信息用于指示第一终端设备与第二终端设备不支持互相通信。

- 10 可选的，处理模块 802，用于根据第一终端设备的安全参数和第二终端设备的安全参数是否匹配，确定第一终端设备和第二终端设备是否支持互相通信，包括：用于当第一终端设备的安全参数和第二终端设备的安全参数匹配时，确定第一终端设备和第二终端设备支持互相通信。

可选的，收发模块 801，还用于发送第二指示信息，第二指示信息用于指示第一终端设备和第二终端设备支持互相通信。

- 15 可选的，收发模块 801，还用于向第一终端设备发送发现响应，发现响应包括业务发现使用的发现参数。

可选的，收发模块 801，还用于向第一终端设备发送第一终端设备的安全参数。

- 20 可选的，安全参数包括安全能力；处理模块 802，用于获取第一终端设备的安全参数，包括：用于通过收发模块 801，接收来自对应的移动管理网元的第一终端设备的安全能力；或者，用于通过收发模块 801，接收来自第一终端设备的第一终端设备的安全能力。

- 25 可选的，安全参数包括安全策略；处理模块 802，用于获取第一终端设备的安全参数，包括：用于通过收发模块 801 接收来自第一终端设备的第一终端设备的安全策略；或者，用于通过收发模块 801 从对应的策略控制网元获取第一终端设备的安全策略；或者，用于通过收发模块 801 从对应的统一数据管理网元获取第一终端设备的安全策略。

其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再赘述。

- 30 在本实施例中，该通信装置 80 以采用集成的方式划分各个功能模块的形式来呈现。这里的“模块”可以指特定 ASIC，电路，执行一个或多个软件或固件程序的处理器和存储器，集成逻辑电路，和/或其他可以提供上述功能的器件。在一个简单的实施例中，本领域的技术人员可以想到该通信装置 80 可以采用图 3 所示的通信设备 300 的形式。

比如，图 3 所示的通信设备 300 中的处理器 301 可以通过调用存储器 303 中存储的计算机执行指令，使得通信设备 300 执行上述方法实施例中的通信方法。

- 35 具体的，图 8 中的收发模块 801 和处理模块 802 的功能/实现过程可以通过图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的计算机执行指令来实现。或者，图 8 中的处理模块 802 的功能/实现过程可以通过图 3 所示的通信设备 300 中的处理器 301 调用存储器 303 中存储的计算机执行指令来实现，图 8 中的收发模块 801 的功能/实现过程可以通过图 3 中所示的通信设备 300 中的通信接口 304 来实现。

由于本实施例提供的通信装置 80 可执行上述通信方法, 因此其所能获得的技术效果可参考上述方法实施例, 在此不再赘述。

需要说明的是, 以上模块或单元的一个或多个可以软件、硬件或二者结合来实现。当以上任一模块或单元以软件实现的时候, 所述软件以计算机程序指令的方式存在, 并被存储在存储器中, 处理器可以用于执行所述程序指令并实现以上方法流程。该处理器可以内置于 SoC (片上系统) 或 ASIC, 也可是一个独立的半导体芯片。该处理器内处理用于执行软件指令以进行运算或处理的核外, 还可进一步包括必要的硬件加速器, 如现场可编程门阵列 (field programmable gate array, FPGA)、PLD (可编程逻辑器件)、或者实现专用逻辑运算的逻辑电路。

当以上模块或单元以硬件实现的时候, 该硬件可以是 CPU、微处理器、数字信号处理 (digital signal processing, DSP) 芯片、微控制单元 (microcontroller unit, MCU)、人工智能处理器、ASIC、SoC、FPGA、PLD、专用数字电路、硬件加速器或非集成的分立器件中的任一个或任一组合, 其可以运行必要的软件或不依赖于软件以执行以上方法流程。

可选的, 本申请实施例还提供了一种通信装置 (例如, 该通信装置可以是芯片或芯片系统), 该通信装置包括处理器, 用于实现上述任一方法实施例中的方法。在一种可能的实现方式中, 该通信装置还包括存储器。该存储器, 用于保存必要的程序指令和数据, 处理器可以调用存储器中存储的程序代码以指令该通信装置执行上述任一方法实施例中的方法。当然, 存储器也可以不在该通信装置中。该通信装置是芯片系统时, 可以由芯片构成, 也可以包含芯片和其他分立器件, 本申请实施例对此不作具体限定。

在上述实施例中, 可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件程序实现时, 可以全部或部分地以计算机程序产品的形式来实现。该计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行计算机程序指令时, 全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中, 或者从一个计算机可读存储介质向另一个计算机可读存储介质传输, 例如, 所述计算机指令可以从一个网站站点、计算机、服务器或者数据中心通过有线 (例如同轴电缆、光纤、数字用户线 (digital subscriber line, DSL)) 或无线 (例如红外、无线、微波等) 方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可以用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质 (例如, 软盘、硬盘、磁带), 光介质 (例如, DVD)、或者半导体介质 (例如固态硬盘 (solid state disk, SSD)) 等。

尽管在此结合各实施例对本申请进行了描述, 然而, 在实施所要求保护的本申请过程中, 本领域技术人员通过查看所述附图、公开内容、以及所附权利要求书, 可理解并实现所述公开实施例的其他变化。在权利要求中, “包括” (comprising) 一词不排除其他组成部分或步骤, “一”或“一个”不排除多个的情况。单个处理器或其他单元可以实现权利要求中列举的若干项功能。相互不同的从属权利要求中记载了某些措施,

但这并不表示这些措施不能组合起来产生良好的效果。

- 5 尽管结合具体特征及其实施例对本申请进行了描述，显而易见的，在不脱离本申请的精神和范围的情况下，可对其进行各种修改和组合。相应地，本说明书和附图仅仅是所附权利要求所界定的本申请的示例性说明，且视为已覆盖本申请范围内的任意和所有修改、变化、组合或等同物。显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求 书

1、一种通信方法，其特征在于，所述方法包括：

第一直连通信发现名称管理功能网元获取第一终端设备的安全参数，所述安全参数为建立所述第一终端设备与第二终端设备之间的 PC5 连接所需的安全参数；

5 所述第一直连通信发现名称管理功能网元接收来自第二直连通信发现名称管理功能网元的所述第二终端设备的所述安全参数；

所述第一直连通信发现名称管理功能网元根据所述第一终端设备的安全参数和所述第二终端设备的所述安全参数是否匹配，确定所述第一终端设备和所述第二终端设备是否支持互相通信。

10 2、根据权利要求 1 所述的方法，其特征在于，所述第一直连通信发现名称管理功能网元根据所述第一终端设备的安全参数和所述第二终端设备的所述安全参数是否匹配，确定所述第一终端设备和所述第二终端设备是否支持互相通信，包括：

当所述第一终端设备的安全参数和所述第二终端设备的所述安全参数不匹配时，所述第一直连通信发现名称管理功能网元确定所述第一终端设备和所述第二终端设备
15 不支持互相通信。

3、根据权利要求 2 所述的方法，其特征在于，所述方法还包括：

所述第一直连通信发现名称管理功能网元发送第一指示信息，所述第一指示信息用于指示所述第一终端设备与所述第二终端设备不支持互相通信。

20 4、根据权利要求 1 所述的方法，其特征在于，所述第一直连通信发现名称管理功能网元根据所述第一终端设备的安全参数和所述第二终端设备的所述安全参数是否匹配，确定所述第一终端设备和所述第二终端设备是否支持互相通信，包括：

当所述第一终端设备的安全参数和所述第二终端设备的所述安全参数匹配时，所述第一直连通信发现名称管理功能网元确定所述第一终端设备和所述第二终端设备支持互相通信。

25 5、根据权利要求 4 所述的方法，其特征在于，所述方法还包括：

所述第一直连通信发现名称管理功能网元发送第二指示信息，所述第二指示信息用于指示所述第一终端设备和所述第二终端设备支持互相通信。

6、根据权利要求 4 所述的方法，其特征在于，所述方法还包括：

30 所述第一直连通信发现名称管理功能网元向所述第一终端设备发送发现响应，所述发现响应包括业务发现使用的发现参数。

7、根据权利要求 1-6 任一项所述的方法，其特征在于，所述方法还包括：

所述第一直连通信发现名称管理功能网元向所述第一终端设备发送所述第一终端设备的安全参数。

35 8、根据权利要求 1-7 任一项所述的方法，其特征在于，所述安全参数包括安全策略，和/或安全能力。

9、根据权利要求 8 所述的方法，其特征在于，所述安全参数包括安全能力；所述第一直连通信发现名称管理功能网元获取所述第一终端设备的安全参数，包括：

所述第一直连通信发现名称管理功能网元接收来自对应的移动管理网元的所述第一终端设备的安全能力；或者，

所述第一直连通信发现名称管理功能网元接收来自所述第一终端设备的所述第一终端设备的安全能力。

10、根据权利要求 8 所述的方法，其特征在于，所述安全参数包括安全策略；所述第一直连通信发现名称管理功能网元获取第一终端设备的安全参数，包括：

5 所述所述第一直连通信发现名称管理功能网元接收来自所述第一终端设备的所述第一终端设备的安全策略；或者，

所述所述第一直连通信发现名称管理功能网元从对应的策略控制网元获取所述第一终端设备的安全策略；或者，

10 所述所述第一直连通信发现名称管理功能网元从对应的统一数据管理网元获取所述第一终端设备的安全策略。

11、根据权利要求 8-10 任一项所述的方法，其特征在于，所述安全策略包括所述 PC5 连接中的用户面机密性保护策略和完整性保护策略；

所述安全能力包括所述 PC5 连接中支持的一个或者多个机密性保护算法和完整性保护算法。

15 12、一种第一直连通信发现名称管理功能网元，其特征在于，所述第一直连通信发现名称管理功能网元包括：处理模块和收发模块；

所述处理模块，用于获取第一终端设备的安全参数，所述安全参数为建立所述第一终端设备与第二终端设备之间的 PC5 连接所需的安全参数；

20 所述收发模块，用于接收来自第二直连通信发现名称管理功能网元的所述第二终端设备的所述安全参数；

所述处理模块，还用于根据所述第一终端设备的安全参数和所述第二终端设备的所述安全参数是否匹配，确定所述第一终端设备和所述第二终端设备是否支持互相通信。

25 13、根据权利要求 12 所述的第一直连通信发现名称管理功能网元，其特征在于，所述处理模块，用于根据所述第一终端设备的安全参数和所述第二终端设备的所述安全参数是否匹配，确定所述第一终端设备和所述第二终端设备是否支持互相通信，包括：

用于当所述第一终端设备的安全参数和所述第二终端设备的所述安全参数不匹配时，确定所述第一终端设备和所述第二终端设备不支持互相通信。

30 14、根据权利要求 13 所述的第一直连通信发现名称管理功能网元，其特征在于，所述收发模块，还用于发送第一指示信息，所述第一指示信息用于指示所述第一终端设备与所述第二终端设备不支持互相通信。

35 15、根据权利要求 12 所述的第一直连通信发现名称管理功能网元，其特征在于，所述处理模块，用于根据所述第一终端设备的安全参数和所述第二终端设备的所述安全参数是否匹配，确定所述第一终端设备和所述第二终端设备是否支持互相通信，包括：

用于当所述第一终端设备的安全参数和所述第二终端设备的所述安全参数匹配时，确定所述第一终端设备和所述第二终端设备支持互相通信。

16、根据权利要求 15 所述的第一直连通信发现名称管理功能网元，其特征在于，

所述收发模块，还用于发送第二指示信息，所述第二指示信息用于指示所述第一终端设备和所述第二终端设备支持互相通信。

17、根据权利要求 15 所述的第一直连通信发现名称管理功能网元，其特征在于，所述收发模块，还用于向所述第一终端设备发送发现响应，所述发现响应包括业务发现使用的发现参数。

18、根据权利要求 12-17 任一项所述的第一直连通信发现名称管理功能网元，其特征在于，所述收发模块，还用于向所述第一终端设备发送所述第一终端设备的安全参数。

19、根据权利要求 12-18 任一项所述的第一直连通信发现名称管理功能网元，其特征在于，所述安全参数包括安全策略，和/或安全能力。

20、根据权利要求 19 所述的第一直连通信发现名称管理功能网元，其特征在于，所述安全参数包括安全能力；所述处理模块，用于获取所述第一终端设备的安全参数，包括：

用于通过所述收发模块，接收来自对应的移动管理网元的所述第一终端设备的安全能力；或者，

用于通过所述收发模块，接收来自所述第一终端设备的所述第一终端设备的安全能力。

21、根据权利要求 19 所述的第一直连通信发现名称管理功能网元，其特征在于，所述安全参数包括安全策略；所述处理模块，用于获取第一终端设备的安全参数，包括：

用于通过所述收发模块接收来自所述第一终端设备的所述第一终端设备的安全策略；或者，

用于通过所述收发模块从对应的策略控制网元获取所述第一终端设备的安全策略；或者，

25 用于通过所述收发模块从对应的统一数据管理网元获取所述第一终端设备的安全策略。

22、根据权利要求 19-20 任一项所述的第一直连通信发现名称管理功能网元，其特征在于，所述安全策略包括所述 PC5 连接中的用户面机密性保护策略和完整性保护策略；

30 所述安全能力包括所述 PC5 连接中支持的一个或者多个机密性保护算法和完整性保护算法。

23、一种通信装置，其特征在于，所述通信装置包括：处理器和接口电路；

所述接口电路，用于接收计算机程序或指令并传输至所述处理器；

35 所述处理器用于执行所述计算机程序或指令，以使所述通信装置执行如权利要求 1-11 中任一项所述的方法。

24、一种计算机可读存储介质，其特征在于，包括计算机程序或指令，当其在通信装置上运行时，使得所述通信装置执行如权利要求 1-11 中任意一项所述的方法。

25、一种通信系统，其特征在于，所述通信系统包括第一直连通信发现名称管理功能网元和第二直连通信发现名称管理功能网元；

所述第一直连通信发现名称管理功能网元，用于获取第一终端设备的安全参数，所述安全参数为建立所述第一终端设备与第二终端设备之间的 PC5 连接所需的安全参数；

5 所述第二直连通信发现名称管理功能网元，用于获取所述第二终端设备的所述安全参数，并向所述第一直连通信发现名称管理功能网元发送所述第二终端设备的所述安全参数；

10 所述第一直连通信发现名称管理功能网元，还用于接收来自所述第二直连通信发现名称管理功能网元的所述第二终端设备的所述安全参数，并根据所述第一终端设备的安全参数和所述第二终端设备的所述安全参数是否匹配，确定所述第一终端设备和所述第二终端设备是否支持互相通信。